

AUDIT PANEL

Day: Tuesday
Date: 29 May 2018
Time: 2.00 pm
Place: Lesser Hall 2 - Dukinfield Town Hall

Item No.	AGENDA	Page No
1.	APOLOGIES FOR ABSENCE To receive any apologies for the meeting from Members of the Panel.	
2.	DECLARATIONS OF INTEREST To receive any declarations of interest from Members of the Panel.	
3.	MINUTES The Minutes of the meeting of the Audit Panel held on 6 March 2018 to be signed by the Chair as a correct record.	1 - 6
4.	REVIEW OF INTERNAL AUDIT 2017/18 To consider the attached report of the Director of Finance.	7 - 22
5.	RISK MANAGEMENT AND AUDIT SERVICE ANNUAL REPORT 2017/18 To consider the attached report of the Head of Risk Management and Audit Services.	23 - 48
6.	ANNUAL GOVERNANCE REPORT 2017/18 To consider the attached report of the Director of Finance and the Head of Risk Management and Audit Services.	49 - 92
7.	RISK MANAGEMENT AND AUDIT SERVICES PLANNED WORK 2018/19 To consider the report of the Head of Risk Management and Audit Services.	93 - 128
8.	INFORMATION GOVERNANCE REPORT To consider the attached report of the Head of Risk Management and Audit Services.	129 - 232
9.	GMPF STATEMENT OF ACCOUNTS 2017-2018 GOVERNANCE ARRANGEMENTS To consider the attached report of the Director of Finance and the Assistant Director of Pensions, Local Investments and Property.	233 - 236

Item No.	AGENDA	Page No
10.	GMPF 2017-18 AUDIT PLAN To consider the attached report of the Director of Finance and the Assistant Director of Pensions, Local Investments and Property.	237 - 254
11.	URGENT ITEMS To consider any additional items the Chair is of the opinion shall be dealt with as a matter of urgency.	

Public Document Pack Agenda Item 3.

AUDIT PANEL

Tuesday, 6 March 2018

Commenced: 2.00 pm

Terminated: 3.10 pm

Present: Councillors Ricci (Chair), Affleck (Deputy Chair), Fairfoull and Peet

In Attendance: Tom Wilkinson Assistant Director of Finance
Wendy Poole Head of Risk Management and Audit Services

Apologies for Absence: Councillors Bailey and K Welsh

16. DECLARATIONS OF INTEREST

There were no declarations of interest.

17. MINUTES

The Minutes of the proceedings of the meeting of the Audit Panel held on 24 October 2017 were agreed and signed as a correct record.

18. GRANT CERTIFICATION LETTER 2016-17

Consideration was given to the Grant Certification Letter for 2016/17, which detailed the results of the Housing Benefit Subsidy Grant Certification work completed in respect of 2016/17.

The letter summarised Grant Thornton's overall assessment of the Council's management arrangements in respect of the certification process. A small number of minor issues had been identified during the process, which had been reviewed and amended accordingly and Grant Thornton had reported their findings to the Department for Work and Pensions.

Details of the Certification fees were also included. It was confirmed that the indicative fee for 2016/17 was based on the final 2014/15 certification fees that reflected the amount of work required by the auditor to certify the Housing Benefit Subsidy Claim from that year. The indicative scale fee charged to the Council was set by Public Sector Audit Appointments Limited.

RESOLVED:
That the report be noted.

19. EXTERNAL AUDIT PLAN 2017-18

Consideration was given to Grant Thornton's External Audit Plan for Tameside Metropolitan Borough Council for the year ending 31 March 2018. The plan provided an overview of the planned scope and timing of the statutory audit of the Council.

Grant Thornton were required to undertake work to enable them to form and express an opinion on the financial statements, including the Annual Governance Statement, that had been prepared by management with the oversight of those charged with governance and Value for Money

arrangements in place at the Council for securing economy, efficiency and effectiveness in the use of resources.

The report outlined any significant risks that had been identified, materiality, Value for Money arrangements and audit logistics including audit fees.

RESOLVED:

That the external audit plan be noted.

20. ACCOUNTING POLICIES AND ESTIMATES FOR 2017/18 ACCOUNTS

The Director of Finance submitted a report, which sought to bring the following items to the attention of the Panel in advance of the closure of the accounts for 2017/18:-

- The proposed accounting policies;
- The critical judgements made in applying the accounting policies; and
- Assumptions made about the future and other major sources of estimated uncertainty within the accounts.

The accounting policies, published within the Statement of accounts in accordance with International Financial Reporting Standards, were used to produce the financial statement for 2017/18 and were appended to the report.

Judgements applied in the accounting policies of the Council when preparing the accounts were detailed and included accounting for schools (balance sheet recognition of schools and transfers to academy status), investment properties, property plant and equipment, business rates, debt impairment, leases, Private Finance Initiatives and similar arrangements, funding, provisions, pensions fund liability, Manchester Airports Group, housing benefit subsidy, reserves and minimum revenue provision.

RESOLVED:

- (i) **That the Statement of Accounting Policies, as appended to the report, be approved;**
- (ii) **That approval be given to management's assessment that the preparation of the accounts on a going concern basis was appropriate; and**
- (iii) **That the critical judgements and major sources of estimated uncertainties be noted.**

21. GRANT THORNTON ASSURANCE

The Director of Finance submitted a report, which explained that Grant Thornton, as part of their risk assessment procedures, were required to obtain an understanding of management processes in relation to fraud risk assessment, laws and regulations and going concern consideration as part of their annual audit.

The report presented the response to the letters and questionnaires received from Grant Thornton for consideration by the Panel ahead of the document being signed by the Chair of the Panel and the Director of Finance.

RESOLVED:

- (i) **That the content of the report and the responses detailed in Appendices A and B to the report, be noted; and**
- (ii) **That the schedule be signed by the Chair of the Panel and the Director of Finance.**

22. CIPFA FRAUD AND CORRUPTION TRACKER

The Director of Finance submitted a report, which advised Members of the report produced by the Chartered Institute of Public Finance and Accountancy Counter Fraud Centre – Fraud and Corruption Tracker 2017 for Tameside.

It was reported that the Chartered Institute of Public Finance and Accountancy Counter Fraud Centre led and coordinated the fight against fraud and corruption across public services by providing a one-stop-shop for thought leadership, counter fraud tools, resources and training.

The report detailed the results of the 2016/17 survey and compared Tameside to other Metropolitan Unitaries and focused on common fraud types specific to local authorities. Details of the type of fraud along with the number of cases and values were provided. The top four types of fraud were housing and tenancy, council tax, insurance claims and procurement. For Tameside there were 1,299 cases of council tax fraud, 4 cases of adult social care fraud, 2 cases of school funds fraud and 1 case of economic and voluntary sector fraud. The number of frauds dealt with was low and because of the nature of investigations and the definition of “Detected Fraud” very little was reported in the survey.

It was estimated that across local authorities more than 75,000 frauds had been detected or prevented in 2016/17 with a total value of £336.2 million. Procurement, adult social care and council tax single person discount were perceived to be the three greatest fraud risk areas, with adult social care having the largest increase over the last year.

As a result of the survey the Chartered Institute of Public Finance and Accountancy had made the following recommendations to organisations:-

- Ensure that cyber security was integral to any new strategy or policy decision, reflecting the National Cyber Security Strategy 2016 to 2021;
- Continue to be vigilant and raise awareness of fraud within adult social care;
- Have a strong counter fraud leadership that understood the importance of involving counter fraud practitioners when devising policy and strategy;
- Continue to maximise opportunities to share data and explore innovative use of data within the law; and
- Communicate clearly the role of the fraud team and the importance of the role for both financial and reputational benefit.

The report would be used to inform the work plan of the Risk Management and Audit Team for 2018/19 in terms of proactive fraud work and the Internal Audit Plan in order to ensure robust controls were in place within systems to minimise future occurrence of known frauds.

Members requested that for future years a comparison be provided against the previous year’s data for Tameside.

RESOLVED:

That the report be noted.

23. RISK MANAGEMENT

The Director of Finance submitted a report detailing the Risk Management Policy and Strategy for 2018/2020 and the Corporate Risk Register, copies of which were appended to the report.

It was explained that risk management was facilitated by the Risk Management and Audit Service and risks were owned by members of the Single Leadership Team, with support from Assistant

Directors, managers and staff. The Single Leadership Team had been consulted with and their comments had been incorporated into the updated risk register.

It was reported that the Risk Management Policy and Strategy had been reviewed and updated with updates relating to Risk Management Guidelines, which had been simplified and duplicated information removed. The Corporate Risk Register had been updated to reflect recent changes to the management structure in January 2018. Following the liquidation of Carillion on 15 January 2018, the risk of the new college and joint public service centre in Ashton not being completed within time and budget had been added to the register. The risk of an increase of illegal dumping of waste on public and private land within the borough had also been added to the register. In addition, a number of risks had been amended as follows:-

- The risk rating for failure to reconcile Guaranteed Minimum Pensions data prior to the HMRC deadline of 2018 had been reduced to 4.
- The risk rating for requirements of the Care Act on service provision and associated financial implications had been reduced to 8.
- The risk rating for failure to reduce demand upon Children's Social Care had been increased to 15.

The risk relating to the impact on service delivery of organisational restructuring and loss of staff had been removed from the register.

The Corporate Risk Register would continue to be presented to the Single Leadership Team on a regular basis with updates provided to the Panel. The process for producing risk registers would be reviewed in conjunction with Tameside and Glossop Clinical Commissioning Group over the coming months to assess the most effective process for compiling and maintaining risk registers and to ensure that available resources were used effectively.

RESOLVED:

- (i) **That the Risk Management Policy and Strategy be approved; and**
- (ii) **That the Corporate Risk Register be approved.**

24. PROGRESS REPORT ON RISK MANAGEMENT AND AUDIT ACTIVITIES APRIL 2017 TO 2 FEBRUARY 2018

The Director of Finance submitted a report detailing the work undertaken by the Risk Management and Internal Audit Service in-between April 2017 to 2 February 2018 in respect of the approved Plan for 2017/18.

The key priorities for the Risk Management and Insurance team during 2017/18 were detailed as follows:-

- To review the risk management system to ensure that it complied with best practice but was still practical for use by the organisation;
- To facilitate the delivery of risk workshops to enable both the Corporate Risk Register to be updated and Operational Risk Registers to be maintained by managers;
- To facilitate the continued implementation of the Information Governance Framework and prepare for the introduction of the General Data Protection Regulations in May 2018;
- To review the Business Continuity Management system in place to streamline the process to create a management tool that was workable, with the capability to provide knowledge and information should a major incident occur affecting service delivery; and
- To continue to support managers to assess their risks as services were redesigned to ensure that changes to systems and procedures remained robust and resilient offering cost effective mitigation and that claims for compensation could be successfully repudiated and defended should litigation occur.

Panel Members were notified that progress to review the risk management process had been delayed due to capacity issues and conflicting priorities. A review would be undertaken in the coming months in conjunction with Tameside and Glossop Clinical Commissioning Group. Work had focused on the information governance agenda in light of the introduction of the General Data Protection Regulations, which would become effective in May 2018 together with the new Data Protection Act.

It was reported that a redesign of the team proposed the deletion of two existing posts (Risk and Insurance Manager and Risk and Insurance Officer), which would be replaced with two Risk Insurance and Information Officers. Recruitment to the posts was currently underway. Work was ongoing in terms of insurance renewal to meet the deadline of 31 March 2018.

With regard to Internal Audit, reference was made to the Audit Plan, which had been approved in May 2017 and covered the period April 2017 to March 2018. An update on progress against the plan to 2 February 2018 was provided. It was reported that 83% of the audit plan had been achieved so far, which was an increase on previous years. It was explained that a detailed review of the audit plan had been undertaken in conjunction with senior management and the original plan of 1,666 days had been revised to 1,479 days with 185 days rescheduled for 2018/19.

During the period October 2017 to February 2018, five final reports were issued in relation to systems, risk and managed audits. In addition, five draft reports had been issued for management review and responses and these would be reported to the Panel in due course. Three school audits were completed during the period, the results of which were summarised. In addition, two further audits had been completed and the draft reports had been issued to the Schools for management review and responses. Eleven Post Audit Reviews had been completed during the period, taking the total to 23 for the year to date, and a further 19 were in progress.

It was reported that the review of Internal Audit against the Public Sector Internal Auditing Standards highlighted that the service was fully compliant with the requirements of the standard. The Public Sector Internal Auditing Standards, introduced from April 2013, required at Standard 1312 that each organisation's internal audit service was subject to an external assessment "once every five years by a qualified, independent assessor or assessment team from outside the organisation". The Peer Review for the Council would be conducted by Blackpool and Bolton and take place from 12 - 14 March 2018.

The Internal Audit Charter for 2018/19 had been refreshed and was appended to the report. It covered definition, responsibility and objectives of internal audit, independence and scope of internal audit, opinion work, reporting internal audit access right and resources.

An update was given on the annual governance statement development areas as follows:-

- Children's Services
- Risk Management and Business Continuity Planning
- Health and Safety
- Managing Change
- Care Together
- Vision Tameside
- Pension Fund Pooling of Investments

An update was also provided on work undertaken on National Anti-Fraud Network Data and Intelligence Services.

With regard to Irregularities / Counter Fraud Work a summary of cases, which had been investigated during the period, was provided. In total, 21 cases had been received with 14 still under investigation. A table detailing the fraud type, number of cases, value, the amount recovered to date and potential annual savings was outlined.

In relation to Local Audit and Accountability Act 2014, Mazars LLP had been appointed as the Council's new external auditor from 2018/19 until 2022/23. The Council would work with both the existing auditors, Grant Thornton, and Mazars to ensure a smooth transition took place.

RESOLVED:



That the report and performance of the Service Unit for the period April 2017 to 2 February 2018 be noted.

25. URGENT ITEMS

There were no urgent items.

CHAIR

Agenda Item 4.

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officer:	Kathy Roe – Director of Finance
Subject:	REVIEW OF INTERNAL AUDIT 2017/18
Report Summary:	The report reviews the effectiveness of Internal Audit and measures practices and performance of the Internal Audit function with the standards set out in the Public Sector Internal Audit Standards which contributes to the overall effectiveness of the system of internal control.
Recommendations:	That the report be noted.
Links to Community Strategy:	Internal Audit supports the individual operations, which deliver the objectives within the Corporate Plan.
Policy Implications:	Effective Internal Audit supports the achievement of Council objectives and demonstrates a commitment to high standards of corporate governance.
Financial Implications: (Authorised by the Section 151 Officer)	Effective Internal Audit assists in safeguarding assets, ensuring the best use of resources and the effective delivery of services.
Legal Implications: (Authorised by Borough Solicitor)	Demonstrates compliance with the Accounts and Audit Regulations 2015, which require the Council to “undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance”. It also must conduct a review of “the effectiveness of the system of internal control annually”.
Risk Management:	Assists in providing the necessary levels of assurance that the significant risks relating to Council operations are being effectively managed.
Access to Information:	<p>The background papers relating to this report can be inspected by contacting the Report Author, Ian Duncan, Assistant Executive Director (Finance) by contacting:</p> <p> Telephone: 0161 342 3864</p> <p> e-mail: ian.duncan@tameside.gov.uk</p>

1. INTRODUCTION

- 1.1 The purpose of this report is to provide the Audit Panel with the background to the review of Internal Audit, the requirements of the Public Sector Internal Audit Standards, the process that has been adopted and details of the review itself.
- 1.2 It is the responsibility of the Council to conduct the annual review of the effectiveness of the system of internal control in accordance with the Accounts and Audit Regulations 2015 as detailed below and the review of internal audit is one element of the assurance process in place that culminates in the production of the Annual Governance Statement referred to in section 1.5.

1.3 Part 2, Section 3 – Responsibility for Internal Control

A relevant authority must ensure that it has a sound system of internal control which:

- (a) facilitates the effective exercise of its functions and the achievement of its aims and objectives;
- (b) ensures that the financial and operational management of the authority is effective; and
- (c) includes effective arrangements for the management of risk.

1.4 Part 2, Section 5 – Internal Audit

- (1) A relevant body must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account Public Sector Internal Auditing Standards or guidance.
- (2) Any officer or member of a relevant body must, if required to do so for the purpose of the internal audit:
 - (a) Make available such documents and records; and
 - (b) Supply such information and explanation; as are considered necessary by those conducting the internal audit.
- (3) In this regulation “documents and records” includes information recorded in an electronic form.

This is supported by the Council’s Financial Regulations, which reflect Internal Audit’s statutory authority to review and investigate all areas of the Council’s activities in order to ensure that the Council’s interests are protected.

1.5 Part 2 Section 6 – Review of Internal Control System

- (1) A relevant authority must, each financial year:
 - (a) conduct a review of the effectiveness of the system of internal control required by regulation 3; and
 - (b) prepare an Annual Governance Statement.
- (2) If the relevant authority referred to in paragraph (1) is a Category 1 authority (Tameside MBC falls into this category), following the review, it must:
 - (a) consider the findings of the review required by paragraph (1)(a):
 - (i) by a committee; or
 - (ii) by members of the authority meeting as a whole; and
 - (b) approve the Annual Governance Statement prepared in accordance with paragraph (1)(b) by resolution of:
 - (i) a committee; or
 - (ii) members of the authority meeting as a whole.
- (3) (Excluded as this clause relates to category 2 authorities and the Council is a category 1.)
- (4) The Annual Governance Statement, referred to in paragraph (1)(b) must be:

- (a) approved in advance of the relevant authority approving the statement of accounts in accordance with regulations 9(2)(b) or 12(2)(b) (as the case may be); and
- (b) prepared in accordance with proper practices in relation to accounts(a).

2. INTERNAL AUDIT IN TAMESIDE

- 2.1 The function is managed by the Head of Risk Management and Audit Services who during 2017/18 reported directly to the Assistant Director of Finance (Section 151 Officer) until 30 September 2017 and then the Director of Finance (Section 151 Officer) from 1 October 2017.
- 2.2 Internal Audit now comprises of 9.3 FTE staff that have a range of experience and relevant qualifications, and includes two dedicated Fraud Investigators/Counter Fraud Specialists.
- 2.3 The Internal Audit Service is provided to all Directorates/Service Areas together with schools and a comprehensive list of all auditable areas is maintained within the Audit Management System "Galileo". A detailed Annual Audit Plan is produced at the start of each financial year after consultation with both officers and members. Internal Audit also provides services to the Greater Manchester Pension Fund and the Greater Manchester Debt Administration Fund.

3. ASSESSMENT AGAINST THE PUBLIC SECTOR INTERNAL AUDIT STANDARDS –

- 3.1 The Public Sector Internal Audit Standards were introduced in April 2013 and comprise a definition of Internal Auditing, a Code of Ethics for Internal Auditors working in the Public Sector and the Standards themselves. The Standards are mandatory for all internal auditors working in the UK public sector.
- 3.2 The definition of Internal Audit is:
"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".
- 3.3 The definition recognises the consultancy work undertaken and emphasises the need to ensure that the audit function is adding value to and improving the organisations operations.
- 3.4 It is recognised in the standards that the provision of assurance work is the primary role for Internal Audit in the UK public sector. The role requires the Chief Internal Auditor to provide an annual internal audit opinion based on an objective assessment of the framework of governance, risk management and control. Consulting services are advisory in nature and are generally performed at the specific request of the organisation with the aim of improving governance, risk management and control and contributing to the overall opinion.
- 3.5 The purpose of the Code of Ethics is to promote an ethical culture in the profession of internal auditing. It extends beyond the definition of internal auditing to include two essential components:-
 - Principles that are relevant to the profession and practice of internal auditing.
 - Rules of conduct that describe behaviour norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors. There are four principles:-

- **Integrity** – the integrity of internal auditors establishes trust and thus provides the basis of reliance on their judgement.
- **Objectivity** – internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. They make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgements.
- **Confidentiality** – internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
- **Competency** – internal auditors apply the knowledge, skills and experience needed in the performance of internal auditing services.

3.6 The standards themselves are divided into two categories:-

- Attribute Standards – Purpose, Authority and Responsibility.
- Performance Standards – Managing the Internal Audit Activity.

3.7 Table 1 shows the individual standards within the above two categories.

Table 1 – Assessment against the Public Sector Internal Audit Standards – 2017

STANDARDS
ATTRIBUTE
1000 – Purpose, Authority and Responsibility
1100 – Independence and Objectivity
1200 – Proficiency and Due Professional Care
1300 – Quality Assurance and Improvement Programme
PERFORMANCE
2000 – Managing the Internal Audit Activity
2100 – Nature of Work
2200 – Engagement Planning
2300 – Performing the Engagement
2400 – Communicating the Results
2500 – Monitoring Progress
2600 – Communicating the Acceptance of Risks

4. PEER REVIEW OF INTERNAL AUDIT

- 4.1 The Peer Review was carried out Blackpool Council and Bolton Council during 12–14 March 2018.
- 4.2 The Standards require that an external assessment of an organisation's internal audit function is carried out once every five years by a qualified, independent assessor or assessment team from outside of the organisation. External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.
- 4.3 The North West Chief Audit Executives' Group (NWCAE) established a 'peer-review' process that is managed and operated by the constituent authorities. This process addresses the requirement of external assessment by 'self-assessment with independent external validation'.

- 4.4 The Peer Review is undertaken in three stages:-
- Pre Review - Self-assessment and supporting documentation provided to review team for desk top review
 - On-site Review - Interviews were conducted with:-
 Chief Executive
 Director of Finance/Assistant Director of Finance
 Director of Governance and Pensions
 Chair of Audit Panel
 Head of Risk Management and Audit
 Principal Auditor
 Senior Auditor
 Auditor
 - Post Review - Review information collated, resolve queries and produce the draft report for comment and then produce the Final Report.
- 4.5 The report attached at **Appendix 1** details the outcome of the review and confirms that Internal Audit conforms overall to the standards.
- 4.6 Five recommendations and three additional development areas have been included in the report and these have all been included in the Quality Assurance and Improvement Plan for 2018/19 which is a later item on the agenda.

5. PERFORMANCE INDICATORS, VALUE ADDED AND FEEDBACK

- 5.1 Internal Audit has three key performance indicators and for 2017/18 all targets were either met or exceeded:
- 93% of Plan Complete (93% in 2016/17 - Target 90%)
 - 90% of Recommendations Implemented (92% in 2016/17 - Target 90%)
 - 100% Customer Satisfaction (94% in 2016/17 - Target 90%)
- 5.2 With regards to Added Value in the annual plan we endeavour to incorporate a mixture of assurance audits and consultancy reviews requested by management to ensure that the service delivers what the organisation requests. Part of our work involves providing independent assurance regarding the implementation of new systems to ensure that the data is migrated correctly and that the control environment is satisfactory from the outset and this work is valued by managers. During 2017/18 we worked with Exchequer Services, Children's and Resource Management on the following projects:
- UK Mail
 - Tapestry – Early Years System
 - Agresso
 - Oxygen – Supplier Discounts for Early Payment
- 5.3 Furthermore, we get involved in service redesigns and providing advice and support to the process, as it is more efficient and effective if we can ensure that controls are in place at the outset rather than auditing after the event and then finding issues and concerns.
- 5.4 Customer feedback is very positive and can be demonstrated in many ways:-
- Customer satisfaction is very high at 100%, which signifies that auditees appreciate the process, albeit, sometimes they do not like the outcome, especially if a low level of assurance is given;
 - At the planning stage requests for work always outweighs resources available;
 - In year we receive a significant number of requests for advice and support; and
 - In year we receive requests to get involved in new projects.
 - The feedback from the Peer Review was very positive from senior officers interviewed.

- 5.5 The performance of the wider organisation is monitored by the team as we keep a watching brief over the changing profile of risks affecting service delivery from a variety of sources. Through consultation with Executive Members/Senior Managers, facilitating the Information Governance Group, fraud briefings/bulletins and attending AGMA Groups a wealth of intelligence is amassed which enables the internal audit plan and approach to be adapted to keep pace with the changing complexities of local government.
- 5.6 Clearly, an important input into the review of Internal Audit is the view of our External Auditors and a good working relationship is in place and no negative feedback has been received.

6. MANAGING THE RISK OF FRAUD AND CORRUPTION

- 6.1 The Chartered Institute of Public Finance and Accountancy issued, via its Counter Fraud Centre, a Code of Practice in 2014 entitled “Code of Practice on Managing the Risk of Fraud and Corruption”.
- 6.2 The self-assessment has been reviewed and the work of Internal Audit in terms of proactive and reactive fraud work does provide assurance that the requirements of the code are being adhered to. This in turn provides evidence for the assessment of Internal Audit against the Public Sector Internal Auditing Standards.

7. CIPFA STATEMENT ON THE ROLE OF THE HEAD OF INTERNAL AUDIT (HIA)

- 7.1 The Statement sets out the five principles that define the core activities and behaviours that belong to the role of the HIA in public service organisations and the organisational arrangements needed to support them. Successful implementation of each of the principles requires the right ingredients in terms of:
- the organisation;
 - the role; and
 - the individual.

For each principle, the Statement sets out the governance arrangements required within an organisation to ensure that HIA's are able to operate effectively and perform their core duties. The Statement also sets out the core responsibilities of the HIA. Summaries of personal skills and professional standards then detail the leadership skills and technical expertise organisations can expect from their HIA.

- 7.2 The five principles are as follows:-
- The HIA in a public service organisation plays a critical role in delivering the organisation's strategic objectives by championing best practice in governance, objectively assessing the adequacy of governance and management of existing risks, commenting on responses to emerging risks and proposed developments;
 - The HIA in a public service organisation plays a critical role in delivering the organisation's strategic objectives by giving an objective and evidence based opinion on all aspects of governance, risk management and internal control;
 - The HIA in a public service organisation must be a senior manager with regular and open engagement across the organisation, particularly with the Leadership Team and with the Audit Committee;
 - The HIA in a public service organisation must lead and direct an internal audit service that is resourced to be fit for purpose; and
 - The HIA in a public service organisation must be professionally qualified and suitably experienced.

- 7.3 A self-assessment has been undertaken against the checklist published in the report by the Chartered Institute of Public Finance and Accountancy (CIPFA) on the role of the Head of Internal Audit as part of the review of the system of internal audit and the Head of Internal Audit is in full compliance with the five principles and the supporting standards.

8. AUDIT PANEL

- 8.1 The system of internal control includes the role of the Audit Panel and, in particular, it's role in the receipt and evaluation of reports from the Head of Risk Management and Audit Services, both in terms of assurance opinions and in ensuring that appropriate arrangements are in place to evaluate and improve the effectiveness of risk management, control and governance processes across the Council. It has operated in accordance with best practice and guidance from the Chartered Institute of Public Finance and Accountancy for 2017/18.

9. CONCLUSIONS

- 9.1 The Peer Review conducted in March 2018 confirms that Internal Audit conforms to the requirements of the Public Sector Internal Audit Standards, as demonstrated in **Appendix 1**.
- 9.2 From the review of Internal Audit, it can be concluded that it helps the organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes in accordance with the Public Sector Internal Auditing Standard's definition. Taking on board the positive comments received from our External Auditors and the positive comments received from Senior Management Teams/Executive Members assurance can be given that the Council has an adequate and effective Internal Audit function which contributes to the overall effectiveness of the system of internal control.

10. RECOMMENDATION

- 10.1 That the report be noted.

This page is intentionally left blank

TAMESIDE METROPOLITAN BOROUGH COUNCIL

**PEER REVIEW OF INTERNAL AUDIT AGAINST THE UK
PUBLIC SECTOR INTERNAL AUDIT STANDARDS**

CARRIED OUT BY

Tracy Greenhalgh – Blackpool Council
Andrew Wright – Bolton Council

SUPPORTED BY

Gary Smith – Blackpool Council

ASSESSMENT DATES: 12 - 14 March 2018
FINAL REPORT DATE: 3 May 2018

Tameside Metropolitan Borough Council

Peer Review of Internal Audit against the UK Public Sector Internal Audit Standards

1 Introduction

- 1.1 All principal local authorities and other relevant bodies subject to the Accounts and Audit (England) Regulations 2015 (amended), the Accounts and Audit (Wales) regulations 2005, section 95 of the Local Government (Scotland) Act 1973 and the Amendment to the Local Government (Accounts and Audit) Regulations (Northern Ireland) 2006 must make provision for internal audit in accordance with the Public Sector Internal Audit Standards (PSIAS) as well as the (CIPFA) Local Government Application Note.
- 1.2 A professional, independent and objective internal audit service is one of the key elements of good governance in local government.
- 1.3 The PSIAS require that an external assessment of an organisation's internal audit function is carried out once every five years by a qualified, independent assessor or assessment team from outside of the organisation. External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.
- 1.4 The North West Chief Audit Executives' Group (NWCAE) has established a 'peer-review' process that is managed and operated by the constituent authorities. This process addresses the requirement of external assessment by 'self-assessment with independent external validation' and this report presents the summary findings of the review carried out on behalf of Tameside Metropolitan Borough Council.
- 1.5 "An independent assessor or assessment team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organisation to which the internal audit activity belongs." This review has been carried out by the Heads of Audit and Risk at Blackpool Council and the Audit Manager at Bolton Council and was supported by the Audit Manager at Blackpool Council. Their 'pen pictures', outlining background experience and qualifications, are included at **Appendix 1**.

2 Approach/Methodology

- 2.1 The NWCAE Group has agreed a detailed Memorandum of Understanding (MoU) that outlines the broad methodology for the conduct of this review. A copy of the MoU is available upon request. However, in summary, the key elements of the process are:
 - The peer review is undertaken in three stages: pre-review; on-site review; post-review and covers audit activity during the period covered in the latest Head of Internal Audit Annual Report & Opinion. For example, reviews commencing after 1 July 2016 will cover the audit year 1 April 2015 to 31 March 2016.
 - Each authority is required to complete and share its self-evaluation of the Internal Audit service together with any relevant supporting evidence/documentation in advance of on-site review commencement. The NWCAE Group has agreed that the self-assessment will use the CIPFA Local Government Application Note (LGAN) questionnaire. Typically, supporting evidence will include the Internal Audit Plan & Charter, the Head of Internal Audit Annual Report & Opinion, Quality Assurance & Improvement Programme and examples of final audit reports.
 - To support the on-site review, a customer survey form will be issued to key personnel within the authority being reviewed.
 - The review itself comprises a combination of 'desktop' and 'actual on-site' review.

- The review cannot reasonably consider all elements of the LGAN self-assessment and the review team must use the 'desktop' period to determine strengths, weaknesses and subsequent key lines of enquiry in order that the review itself is risk-based, timely and adds real value. Each authority will be assessed against the four broad themes of: Purpose and Positioning; Structure and Resources and Audit Execution.
- Upon conclusion, the review team offers a 'true and fair' judgement and it is proposed that each Authority will be appraised as Conforms, Partially Conforms or Does Not Conform against each thematic area of the LGAN, from which an aggregation of the three themed scores gives an overall Authority score.

3 Summary Findings

- 3.1 Following a detailed moderation process, the review team has concluded the following judgements:

Area of Focus	Judgement
Purpose & Positioning	Conforms
Structure & Resources	Conforms
Audit Execution	Conforms
Overall Judgement	Conforms

- 3.2 Assessment against the individual elements of each area of focus is included in the table at **Appendix 2** and a summary of the areas for consideration to improve / develop the service is identified within the action table at **Appendix 3**.
- 3.3 Additional points for consideration identified during the review that are out of scope of the Standards / LAGN requirements but are contributory to the overall effectiveness and efficiency of the internal audit service are presented in the table at **Appendix 4** of the report for information and consideration only.

4 Observations and Recommendations

4.1 Standards

1000 Purpose, Authority and Responsibility

- 4.1.1 It was identified as part of the interviews and questionnaires completed that the internal audit service are valued for how responsive they are to requests to provide advice and support. A recurrent theme was the transformation programme underway at the Council and how internal audit will need to ensure that they are appropriately skilled and flexible to effectively operate in the 'new world' and continue to add value in the future. Overall, the impression was of a well-regarded internal audit service with a good profile and communications within the business.

1110 Organisational Independence

- 4.1.2 No formal process exists for formal feedback to be sought from the Chief Executive or the Chair of Audit Panel to inform the annual appraisal or performance review of the Head of Risk Management and Audit. Whilst we established that informal communications channels exist, a more formal process would facilitate positive feedback as well as any concerns, which are currently only raised on an ad-hoc basis (**Recommendation 1**).

1130 Impairment to Independence or Objectivity

- 4.1.3 A management decision was taken to give the Head of Risk Management and Audit the role of the Senior Information Risk Owner (SIRO). As the nominated SIRO the Head of

Risk Management and Audit owns information governance risks for the Council which impairs the independence required to provide assurance of this function **(Recommendation 2)**.

- 4.1.4 The Head of Risk Management and Audit has operational responsibility for a number of areas including risk management, insurance and fraud. When an audit of these areas is required a procedure is documented to ensure that the Head of Risk Management and Audit maintains independence from the audit process by reporting through the Assistant Director of Finance (Deputy S151 Officer). When interviewed the Assistant Director of Finance (Deputy S151 Officer) had not considered this arrangement as no such audits had taken place in 2017/18. As part of the 2018/19 planning process we have been advised that the Assistant Director of Finance (Deputy Section 151 Officer) has been informed of the process as a number of audits are planned which fall under the remit of the Head of Risk Management and Audit therefore assuring appropriate independence.

2010 Planning

- 4.1.5 There is an extensive risk assessment process within the audit universe section of Galileo which is undertaken to produce the audit plan. As part of the process, Principal Auditors discuss risks with senior managers. However, the audit plan does not:

- Make reference to the corporate risk register nor illustrate how corporate risks drive the audit plan (including the consideration of local and national risks).
- Does not link into the overall assurance framework.
- Demonstrate how the internal audit service links to the Council's objectives and priorities.
- Outline the priorities of each assignment.

To demonstrate that risk based audit planning is undertaken there would be benefits in further developing the internal audit plan to take account of the above bullet points **(Recommendation 3)**.

- 4.1.6 As is common in the local government sector, resource available for the internal audit plan is driven by the number of staff available, not the number of staff required to deliver the overall level of work. Whilst it is accepted that this is the case the audit plan could be more specific to outline what an optimum level of staff would be able to deliver. This would enable the Audit Panel and Senior Management Team to make an informed assessment of the adequacy of staffing levels **(Recommendation 4)**.

1300 Quality Assurance and Improvement Programme

- 4.1.7 A Quality Assurance and Improvement Programme (QAIP) is in place which is updated on an annual basis and presented to Audit Panel in line with the standards. It was noted that no improvement action plan was linked to this to highlight what actions had been identified to drive improvement and enable Audit Panel to monitor the achievement of these **(Recommendation 5)**.

- 4.1.8 Performance indicators are only reported to Audit Panel at year end and it may be beneficial to report these on a more frequent basis to ensure that the Audit Panel are aware of any potential underperforming areas and seek assurance that remedial action is being taken. We understand this has been discussed with the Audit Panel previously and it has been agreed that performance data should continue to be reported annually as mid-year / quarterly reporting can be misleading due to timing issues. We acknowledge that the audit team monitor performance on a much more frequent basis.

Review Team

Andrew Wright (CMIIA / CIPFA)

Andrew is a qualified Chartered Internal Auditor (CMIIA) and Chartered Public Finance Accountant (CPFA). In his career at Bolton Council he has managed the planning and delivery of audit services across the whole range of council services, and has managed the provision of internal audit services to an external housing association client.

In his current role, Andrew is responsible for managing the council's internal audit function, reporting to the Head of Audit and Risk Management for Bolton Council, Manchester City Council and the Greater Manchester Combined Authority.

Tracy Greenhalgh (CMIIA / MSc Audit Management and Consultancy / MSc Counter Fraud and Counter Corruption)

Tracy is a fully qualified member of the Chartered Institute of Internal Auditors and received a commendation in her MSc in Audit Management and Consultancy and a merit in her MSc Counter Fraud and Counter Corruption. Tracy has nineteen years internal audit experience in the local government sector and is currently Head of Audit and Risk at Blackpool Council.

Tracy's oversees the delivery of the audit plans across the full range of Council services and five wholly owned companies. Her wider portfolio includes responsibility for corporate fraud, risk management, insurance, business continuity, emergency planning, health and safety and equality and diversity.

Detailed Assessment

PSIAS Ref		Conforms	Partially conforms	Does not conform	Comments
	Purpose and Positioning				
1000	Remit	X			
1000	Reporting lines	X			
1110 / 1130	Independence		X		Paragraph 4.1.2, Recommendation 1 Paragraph 4.1.3 Recommendation 2
2010	Risk based plan		X		Paragraph 4.1.5, Recommendation 3 Paragraph 4.1.6, Recommendation 4
2050	Other assurance providers	X			
	Structure and Resources				
1200	Competencies	X			
1210	Technical training and development	X			
1220	Resourcing	X			
1230	Performance management	X			
1230	Knowledge management	X			
	Audit Execution				
1300	Quality Assurance and Improvement Programme		X		Paragraph 4.1.7, Recommendation 5
2000	Management of the IA function	X			
2200	Engagement Planning	X			
2300	Engagement delivery	X			
2400	Reporting	X			
2450	Overall opinion	X			

Conforms	X	Partially Conforms	Does Not Conform
-----------------	----------	---------------------------	-------------------------

Tameside Metropolitan Borough Council Internal Audit Service – PSIAS Action Table

The following points for action to develop the Audit Function arise from the review undertaken:



PSIAS Ref	Rec No.	Points for Consideration	Responsible	Action
1110	1	Consideration should be given to obtaining formal feedback from the Chief Executive and Chair of Audit Committee for the annual appraisal of the Head of Risk Management and Audit.	Director of Finance	The Annual Development Review for the Head of Risk Management and Audit will take on board the recommendation made.
1130	2	Consider allocating the formal SIRO designation to a chief officer, even if the internal audit team continues to support the SIRO function.	Director of Finance/Director of Governance and Resources	The roles relating to Information Governance are being discussed at a meeting on 9 May 2018.
2010	3	Consideration should be given to demonstrating how the audit plan and priorities align to the corporate risk register, assurance framework, link to the Council's objectives and priorities and the prioritisation of audit assignments.	Wendy Poole Head of Risk Management and Audit Services	The Audit Plan for 2018/19 will be presented taking on board this recommendation.
2010	4	The audit plan could be more specific to outline what an optimum level of staff would be able to deliver. This would enable the Audit Panel and Senior Management Team to make an informed assessment of the adequacy of staffing levels.	Wendy Poole Head of Risk Management and Audit Services	The planning process for 2018/19 and future years will incorporate the recommendation made.
1300	5	The Quality Assurance and Improvement Programme (QAIP) should include an action plan identifying steps which will be taken to continually improve the service and enable Audit Panel to monitor progress. The Quality Assurance and Improvement Programme should also be referenced in the Annual Report.	Wendy Poole Head of Risk Management and Audit Services	The Quality Assurance and Improvement Programme (QAIP) for 2018/19 will take on board the recommendation and detail the improvements included in this report as a minimum.

Tameside Metropolitan Borough Council Internal Audit Service – Additional Development Action Table

During the review the following additional points for consideration were identified. Whilst these specific points are out of scope of the Standards / LGAN requirements, they are nonetheless contributory to the overall effectiveness and efficiency of the Internal Audit service and are presented in this report for information and consideration only:

Rec No.	Points for Consideration	Responsible	Action
1	The Audit Plan and Progress reports to Audit Panel are described as reports of the AD Finance/Director of Finance with the Head of Risk Management and Audit also listed as a reporting officer. To ensure that audit retains its organisational independence we recommend that the reports go in the name of the Head of Risk Management and Audit.	Wendy Poole Head of Risk management and Audit Services	This will be discussed with the Director of Finance and Director of Governance and Pensions, as normal practice at the Council is for the Director to be listed then the reporting officer.
2	Consideration should be given to identifying the skills needs by the audit team to assist the Council with its current transformation programme and provide training and development opportunities to address any skills shortage.	Wendy Poole Head of Risk management and Audit Services	This will be discussed with the Director of Finance to ensure the appropriate skills are identified and training and development opportunities to address any skills shortage delivered.
3	Clearer guidance on the extent of post audit review work should be documented in line with the number and priority of recommendations. In addition, improved transparency could be achieved by including post audit reviews in the periodic progress reports to Audit Panel. Consideration should also be given to the process for agreeing extensions to target implementation dates and post audit review timings.	Wendy Poole Head of Risk management and Audit Services	Further enhancements to the progress reports to the Audit Panel were introduced during 2017/18 and the recommendation will be considered for the reporting process for 2018/19.

Agenda Item 5.

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officer:	Wendy Poole – Head of Risk Management and Audit Services
Subject:	RISK MANAGEMENT AND AUDIT SERVICES – ANNUAL REPORT 2017/2018
Report Summary:	The report summarises the work performed by the Service Unit and provides assurances as to the adequacy of the Council's systems of internal control.
Recommendations:	Members note the report.
Links to Community Strategy:	Internal Audit supports the individual operations, which deliver the objectives within the Community Strategy.
Policy Implications:	Effective Risk Management and Internal Audit supports the achievement of Council objectives and demonstrates a commitment to high standards of corporate governance.
Financial Implications: (Authorised by the Section 151 Officer)	Effective Risk Management and Internal Audit assists in safeguarding assets, ensuring the best use of resources and the effective delivery of services. It also helps to keep insurance premiums and compensation payments to a minimum.
Legal Implications: (Authorised by the Borough Solicitor)	Demonstrates compliance with the Accounts and Audit Regulations 2015, which require the Council to “undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector auditing standards or guidance”
Risk Management:	The services of the Risk Management and Audit Service Unit assists in providing the necessary levels of assurance that the significant risks relating to the Council's operations are being effectively managed and controlled.
Access to Information:	The background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by contacting:  Telephone: 0161 342 3846  e-mail: wendy.poole@tameside.gov.uk

1 INTRODUCTION

- 1.1 The purpose of the report is to present a review of the Risk Management and Audit Service for 2017/18. It covers Internal Audit, Risk Management and Insurance and the National Anti-Fraud Network (NAFN Data and Intelligence Services).
- 1.2 The definition of Internal Audit is outlined by the Public Sector Internal Audit Standards as follows:
“Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”.
- 1.3 The key elements of the definition are:-
- **Risk Management** – A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation’s objectives.
 - **Control** – Any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organises and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
 - **Governance** – The combination of processes and structures implemented by the Board to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.

2 THE AUTHORITY FOR INTERNAL AUDIT

2.1 Local Government Act 1972 Section 151.

“Every Local Authority shall make arrangements for the proper administration of its financial affairs and shall secure that one of its officers has responsibility for the administration of those affairs”

The Council’s Constitution formally nominates the Director of Finance as the Council’s Section 151 Officer who will rely on the work of the Internal Audit Service for assurance that the Council’s financial systems are operating satisfactorily.

2.2 Accounts and Audit Regulations 2015 Part 2, Section 3 – Responsibility for Internal Control

A relevant Authority must ensure that it has a sound system of internal control which:

- (a) facilitates the effective exercise of its functions and the achievement of its aims and objectives;
- (b) ensures that the financial and operational management of the authority is effective; and
- (c) includes effective arrangements for the management of risk.

2.3 Accounts and Audit Regulations 2015 Part 2, Section 5 – Internal Audit

- (1) A relevant body must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.
- (2) Any officer or member of a relevant body must, if required to do so for the purpose of the internal audit:
 - (a) Make available such documents and records; and
 - (b) Supply such information and explanation;as are considered necessary by those conducting the internal audit.

- (3) In this regulation “documents and records” includes information recorded in an electronic form.

This is supported by the Council’s Financial Regulations, which reflect Internal Audit’s statutory authority to review and investigate all areas of the Council’s activities in order to ensure that the Council’s interests are protected.

2.4 Accounts and Audit Regulations 2015 Section 6 – Review of Internal Control System

- (1) A relevant Authority must, each financial year:
- (a) conduct a review of the effectiveness of the system of internal control required by regulation 3; and
 - (b) prepare an annual governance statement.
- (2) If the relevant Authority referred to in paragraph (1) is a Category 1 Authority, following the review, it must:
- (a) consider the findings of the review required by paragraph (1)(a):
 - (i) by a committee; or
 - (ii) by members of the Authority meeting as a whole; and
 - (b) approve the annual governance statement prepared in accordance with paragraph (1)(b) by resolution of:
 - (i) a committee; or
 - (ii) members of the Authority meeting as a whole.
- (3) Relates to Category 2 Authorities and not applicable to the Council.
- (4) The annual governance statement, referred to in paragraph (1)(b) must be:
- (a) approved in advance of the relevant Authority approving the statement of accounts in accordance with regulations 9(2)(b) or 12(2)(b) (as the case may be); and
 - (b) prepared in accordance with proper practices in relation to accounts(a).

2.5 The Terms of Reference for the Audit Panel adequately meet the requirements of the Accounts and Audit Regulations.

2.6 The review of the effectiveness of the system of internal control referred to in paragraph 2.4 has been conducted and a separate report is on the agenda.

3 KEY ACHIEVEMENTS DURING 2017/2018

- 3.1 The major achievements of the Service Unit for 2017/2018 are as follows: -
- The Internal Audit function was judged to be compliant with the Public Sector Internal Audit Standards (PSIAS) following an External Peer Review in March 2018.
 - The implementation rate for audit recommendations was 90%.
 - Customer feedback is very positive with continued high levels of satisfaction demonstrated on customer questionnaires.
 - Annual reports, plans and regular progress reports presented to Members via the Audit Panel and the Greater Manchester Pension Fund Local Board.
 - The Annual Governance Statement was produced in accordance with best practice and agreed timescales and no adverse comments were received when our External Auditors (Grant Thornton) reviewed it.
 - The National Anti-Fraud Network (NAFN Data and Intelligence Services) delivered its most successful AGM/Summit in London in October 2017, with 249 delegates representing 124 organisations.
 - Twenty three fraud cases were investigated during the year.
 - A School Bursar was charged with three counts of fraud by abuse of position, and after pleading guilty was sentenced to 9 months imprisonment suspended for 12

months and 180 hours unpaid work for misappropriating £19,000 in monies/equipment belonging to the school.

- NAFN received an excellent inspection report from the Investigatory Powers Commissioners Officer (IPCO) in December 2017 with no recommendations received.

4 COVERAGE FOR 2017/2018

- 4.1 The report presented to the Audit Panel on 30 May 2017 provided an overview of the work planned for 2017/2018 for the service unit. The Original Audit Plan of 1666 days was detailed in the report and approved by the Audit Panel. The plan, however, as reported during the year has been revised on a regular basis to ensure that it was aligned to changes in service priorities, risks, directorate structures and resources available.
- 4.2 Table 1 below shows the full year position of the audit plan by Directorate/Service Area. It details the approved plan, the revised plan, the actual days as at 31 March 2018 and the percentage completed. **Appendix 1** provides a detailed breakdown of the 2017/18 Audit Plan.

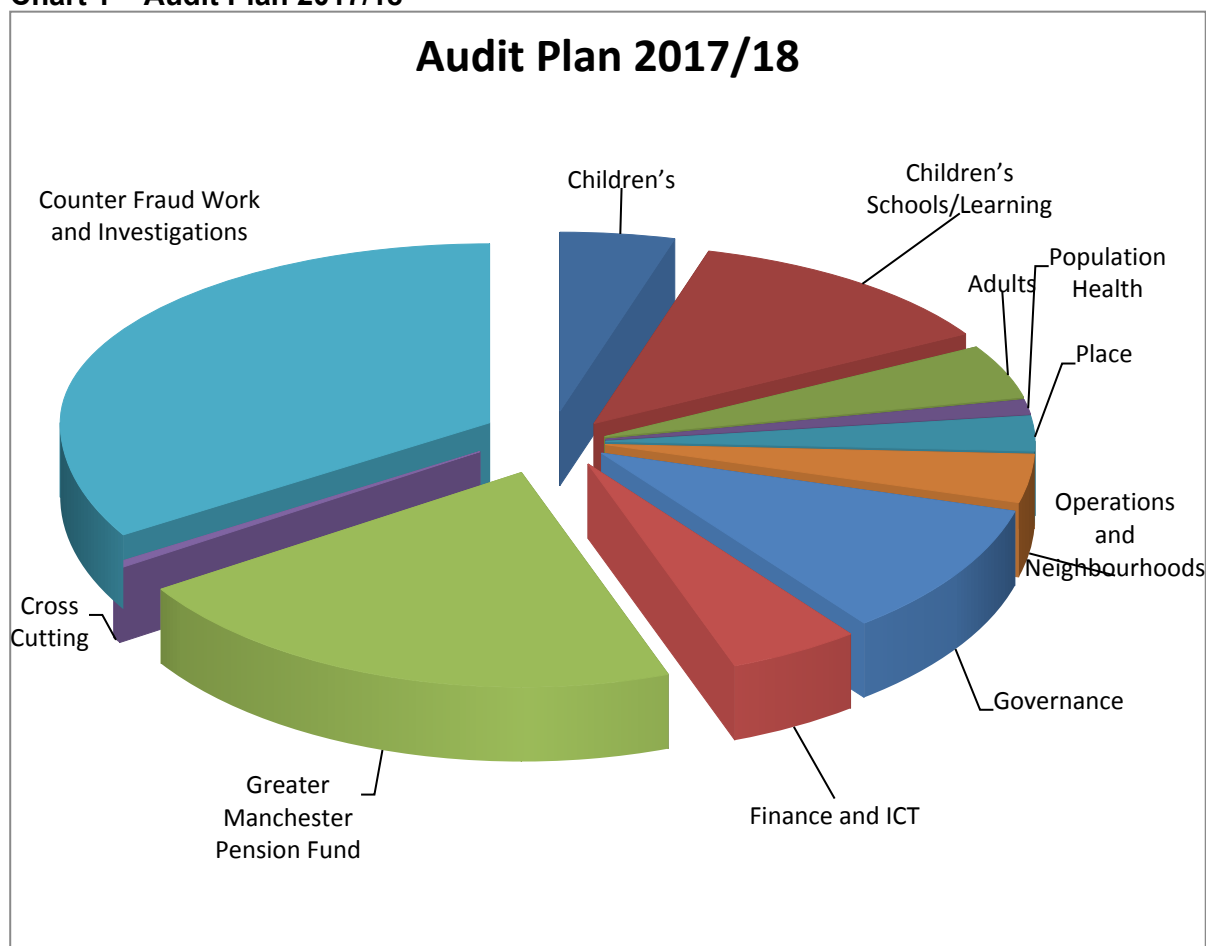
Table 1 – Annual Audit Plan Progress as at 31 March 2018

Service Area / Directorate	Approved Plan Days 2017/18	Revised Plan 2017/18	Actual Days to 31 Mar 2018	%
Adults	59	59	62	105
Children's	117	84	76	90
Population Health	29	29	16	55
Place	62	32	39	112
Operations and Neighbourhoods	98	64	54	84
Governance	156	117	151	129
Finance	100	89	73	82
Learning	205	205	189	92
Cross Cutting	53	23	6	26
Greater Manchester Pension Fund	300	300	318	106
Fraud Work/Irregularity Investigations	487	487	501	103
Total Planned Days for 2017/2018	1,666	1,489	1,485	99.7

- 4.3 Resources on planned work reduced during the year for the following reasons:
- The original plan was based on known estimated resources at the beginning of the year and based on a full complement of staff
 - A significant delay occurred in recruiting an Auditor, the post was vacated in May 2017 and the new appointment joined the team in March 2018. An intensive training and support package has been put in place to enable the new starter to develop as an auditor which will have an impact on productivity in the early months.
 - A number of conflicting priorities in terms of irregularities, which diverted days away from planned work to reactive work to assist with timely responses due the one of the Fraud Investigators/Counter Fraud Specialists leaving in December and not being replaced in March.
 - Responding to requests from managers for new audits and providing advice and support to ensure changes to system, processes and procedures do not adversely affect the control environment.
 - Assisting with and conducting investigations relating to information incidents in line with the Councils Information Security Incidents Reporting Procedure and Practice Note.

- 4.4 The changes resulted in a reduction of 177 planned days from 1,666 to 1,489 and these changes were reported to the Audit Panel in March 2018. In terms of the overall plan, 1,485 actual days were delivered against a revised plan of 1,489. Chart 1 below demonstrates the actual days delivered per Directorate/Service Area.

Chart 1 – Audit Plan 2017/18



- 4.5 The successful delivery of the plan can be measured in two ways:-
- **Actual Productive Audit Days Delivered against the Plan**
The days delivered against the plan, including Fraud Work totalled 1,485 compared to the revised plan of 1,489, which represents 99.7%.
 - **Percentage of Planned Audits Completed**
The second measure focuses on the planned audits, and calculates the actual rate of completion per audit, and then consolidates the individual outcomes into one single percentage figure. The figure for 2017/18 is 93% compared to 93% in 2016/17 and 94% in 2015/16.
- 4.6 This following sections of the report provide details of the key areas covered during the period April 2017 to March 2018 and comment on any important issues arising from our work.
- Financial Systems:**
- 4.7 During 2017/18 seven audits have been undertaken on the financial systems detailed in table 2 to ensure they were operating securely, fit for purpose and that the information generated from them into the general ledger was reliable. Where issues were identified as part of the systems audit work, action plans were agreed with management and these will be followed up in due course:-

Table 2 – Financial Systems Audits 2017/18

Audit	Level of Assurance	Final Issued	Post Audit Review Due
NNDR	Medium	Draft	
Council Tax	Medium	Draft	
VAT	Medium	Draft	
External Audit Assurance Checks	N/A	Feb 2018	N/A
Treasury Management	Medium	Draft	
Payroll	High	Aug 2017	Work In Progress
Creditors	Low	Draft	

- 4.8 Post Audit Reviews have been completed for the General Ledger and Cashiers and the majority of recommendations made have been implemented.
- 4.9 Two financial systems audits were also undertaken on the Pension Fund, as detailed in table 3 below. Where issues were identified as part of the systems audit work, action plans were agreed with management and these will be followed up in due course:-

Table 3 – Financial Systems Audits 2017/18

Audit	Level of Assurance	Final Issued	Post Audit Review Due
Pension Benefits Payable	High	May 2017	Work In Progress
Debtors	Medium	June 2017	Work In Progress

- 4.10 Sections 4.11 to 4.19 provide details of the audit work undertaken in each directorate.
- 4.11 **Adults**
Areas reviewed during the year have included:-
- Reablement;
 - Learning disability Client Accounts;
- 4.12 **Children's**
Areas reviewed during the year have included:-
- Safeguarding
 - Leaving Care
 - Troubled Families
- 4.13 **Population Health**
Areas reviewed during the year have included:-
- Ring-Fenced Public Health Grant
- 4.14 **Place**
Areas reviewed during the year have included:-
- Estates Management Consultancy Review
 - Hattersley Collaboration Agreement
 - Local Growth Fund
- 4.15 **Operations and Neighbourhoods**
Areas reviewed during the year have included:-
- Use of CCTV
 - Local Authority Bus Subsidy Grant
 - Integrated Transport Service
 - Health and Safety

- Cycling Ambition Grant
- Local Transport Capital Block Funding Grant

4.16 Governance

Areas reviewed during the year have included:-

- UK Mail System Sign Off
- Bank Transfer Arrangement Appointeeships/Deputyships;
- Registrars
- Car Allowances Year-End Review
- Oxygen System Sign Off
- Procure to Pay

4.17 Finance

Areas reviewed during the year have included:-

- BACS System Sign Off
- Device Management

4.18 Learning

Areas reviewed during the year have included:-

- ICT Security at Schools

4.19 Greater Manchester Pension Fund:-

Areas reviewed during the year have included:-

- Treasury Management
- First Bus Transfer to GMPF
- Private Equity
- Transfer of Funds to New Credit Manager
- Local Investments Impact portfolio
- Calculation and Payment of Benefits
- Guaranteed Minimum Payments
- Visits to Contributing Bodies
- Review of fund manager Investec
- Greater Manchester Property Venture Fund
- Altair

4.20 A summary of the audit opinions issued in relation to system based audit work for 2017/18 compared to 2016/17 and 2015/16 is shown in Table 4 below: -

Table 4 – Final Reports System Based Audits

Opinion	Total for 2017/18	%	Total for 2016/17	%	Total for 2015/16	%
High	8 (7)	42	5 (4)	20	6 (4)	24
Medium	8 (2)	42	13 (8)	52	14 (3)	56
Low	4 (1)	16	7 (2)	28	5 (0)	20
Totals	20 (10)	100	25 (14)	100	25 (7)	100

Note: The figures in brackets in the above table relate to the Pension Fund

4.21 In addition to the Eighteen final reports issued above, a further fourteen draft reports have been issued for comments and management responses and these will be reported to the Panel in due course.

4.22 Sixteen schools have been audited and final reports issued as part of our cyclical review programme during 2017/2018. A summary of the opinions issued for schools during 2017/2018 compared to 2016/17 and 2015/16 is shown in Table 5 below: -

Table 5 – Audit Opinions – Schools

Opinion	Total for 2017/18	%	Total for 2016/17	%	Total for 2015/16	%
High	8	50	6	50	9	43
Medium	5	31	5	42	7	33
Low	3	19	1	8	5	24
Totals	16	100	12	100	21	100

- 4.23 A further two draft reports have been issued for comments and management responses and these will be reported to the panel in due course.
- 4.24 In addition to the reports issued in Tables 4 and 5, a significant number of days were allocated throughout the year to work that did not generate a report with a level of assurance attached. The reasons for this are:-
- Grant Certification;
 - Advice and consultancy work provided to support service redesigns and the implementation of new or updated systems;
 - Investigating Information Incidents; and
- 4.25 It is important to note, however, that whilst the above work does not generate an audit opinion it undoubtedly adds value to the Council. It ensures that expenditure is in accordance with grant conditions, that new/amended systems are introduced with satisfactory controls in place and that control issues identified as part of irregularity investigations are resolved to improve the control environment.
- 4.26 Thirty Post Audit Reviews have been completed during the year and 90% of agreed recommendations have been implemented. Internal Audit was satisfied with the reasons put forward by management where the recommendations had not been fully implemented. Six related to the Pension Fund, thirteen related to Schools and eleven to Council services/systems.

5 ANTI-FRAUD WORK

Irregularity Investigations

- 5.1 Investigations are conducted by two members of the Internal Audit Team under the direction of a Principal Auditor and the Head of Risk Management and Audit Services to ensure consistency of approach. All cases were investigated using the approved standard protocol and procedure, which complies with best practice. A control report is produced in the majority of cases for management to ensure that corrective action is taken where possible to ensure that the control environment is improved therefore minimising the risk of similar irregularities occurring in the future.
- 5.2 All investigations and assistance cases are reviewed by the Standards Panel every month and where appropriate the members of the Panel challenge and comment on the cases and offer further guidance and direction. Assistance cases can range from obtaining information for an investigating officer to actually undertaking a large proportion of the analysis work to provide evidence for the investigatory process.
- 5.3 The number of cases investigated during the period April 2017 to March 2018 is summarised in Table 6 below.

Table 6 – Investigations Undertaken from April 2017 to March 2018

Detail	No. of Cases
Cases B/Forward from 2016/2017	15
Current Year Referrals	8
Total	23
Cases Closed	12
Cases Still under Investigation	11
Total	23
Assistance Cases	7 (5 Closed)

- 5.4 The above investigations can be categorised by fraud type as shown in Table 7 below.

Table 7 – Investigations by Fraud Type

Fraud Type	No. of Cases	Value £	Recovered To Date £	Potential Annual Savings £
Direct Payment	9	136,114	-	25,058
Procurement/Duplicated Invoices Fraud	2	100,354	To be recovered on retirement - £58,000 (2023)	-
Misappropriation of Monies/Stock	10	20,029	£19,576 – Subject to a Proceeds of Crime Act Hearing	-
Staff Conduct (Time/HB Fraud)	2	1 Proven	-	-
Total	23	256,497		25,058

- 5.5 Seventeen of the above cases investigated involved frauds perpetrated against the Council by claimants or third parties. The figures shown in the Value and Potential Annual Savings column in Table 7, are estimated based on the information available to date. Several of the cases are still being investigated or prepared for prosecution and the value of the fraud could change as the case progresses. The ongoing savings are the value of the Direct Payments that have been stopped because of ongoing investigations.
- 5.6 A School Bursar was charged with three counts of fraud by abuse of position, and after pleading guilty was sentenced to 9 months imprisonment suspended for 12 months and 180 hours unpaid work for misappropriating £19,000 in monies/equipment belonging to the school. The investigation uncovered that the supplier involved was holding unrequired stock on behalf of the school valued at £16,000, an agreement has since been made with the supplier for this money to be spent on items needed by the school.
- 5.7 The processes in place within Internal Audit and across the Council to manage the risk of fraud and corruption are in accordance with the code of practice issued by the Chartered Institute of Public Finance and Accountancy in 2014 entitled “Managing the Risk of Fraud and Corruption”.

National Fraud Initiative

- 5.8 The majority of investigations have now been finalised in relation to the NFI 2016 Data Matching Exercise and Table 8 below summarises the results.

Table 8 – NFI Data Matches 2016

NFI Data Set	Total Number of Matches	Number of Rec'd Matches	Comments		
			Processed	In Progress	No. of Error/Frauds and Value
Pensions to DWP Deceased Persons	849	483	849		1 (F) £16,641
Pensions to Payroll	2,123	614	2,065	58	-
Deferred Pensions to DWP Deceased	87	76	87	-	1 (E)
Housing Benefits to Student Loans	103	29	26	3	0
Housing Benefits Claimants to DWP Deceased	100	60	60	-	-
Council Tax Reduction Scheme to Housing Benefit	85	58	58	-	-
Personal Budgets to DWP Deceased	5	4	5	-	-
Blue Badge to DWP Deceased	43	42	43		35 (E)
Private Residential Cares Homes to DWP Deceased	47	21	39	-	-
Creditors Duplicate Records/Payments	1,441	154	220	2	3 (E) £70,766
Totals	4,883	1,541	3,452	63	1 (F) £16,641 39 (E) £70,766

- 5.9 In summary one fraud was identified totalling £16,641 and thirty nine errors totalling £70,766 were investigated and the monies are being recovered.
- 5.10 Preparations are now underway for the 2018 exercise and the data sets will be submitted to the Cabinet Office in October 2018.

6 NATIONAL ANTI-FRAUD NETWORK (NAFN)

- 6.1 NAFN held its AGM and Summit at The Great Hall, Kensington, London in October and the theme was 'The Changing World of Investigation'. It was an opportunity to celebrate 20 years since NAFN was launched. Overall, the event was the most successful held by NAFN attracting 249 attendees (up 76 on the previous year) representing 124 member organisations (up 35 on last year).
- 6.2 During 2017/18, NAFN has continued to engage with its key stakeholders and members to ensure that the services it offers meet with their requirements and expectations. During the last quarter of the year, the NAFN Executive Board has started to review the strategy for the coming years and a series of meetings are scheduled for May/June 2018 to meet with the Cabinet Office, the Chartered Institute of Environmental Health and the Local Government Association to discuss future plans to enhance service provision.

- 6.3 NAFN was subject to its annual inspection by the Investigatory Powers Commissioners Officer (IPCO) in December and received another positive and successful inspection. No recommendations were received and officers were commended on implementing the previous inspection recommendations and praised for their openness and transparency in recording their actions and cooperating with the inspection.
- 6.4 NAFN continued to work closely with the Local Government Association and Institute of Licensing and will shortly be rolling out a national register of taxi and private hire drivers who have had their licences refused or revoked, improving the safety of the travelling public. It is expected that the register will be operational in May/June 2018.
- 6.5 NAFN exists to support members in their protection of the public purse and acts as an Intelligence Hub providing a single point of contact for members to acquire data and intelligence in support of investigations, enforcement action and debt collection. A breakdown of the membership is provided in Table 9 below:-

Table 9 – NAFN Membership

Member Type	March 2018	March 2017	Target	%
Local Authorities	350	359	418	84
Housing Associations	54	47	N/A	-
Other Public Bodies	14	12	N/A	-
Totals	418	418		

- 6.6 The Marketing Strategy and Plan has continuing to pay dividends as the service is continuing to attract new members from both local authorities and housing associations. Regular marketing emails are sent to all registered users outlining the various services on offer to all members as the subscription provides corporate membership. A programme of webinars offering training and guidance without leaving the office has also proved to be very popular with most sessions being fully booked.
- 6.7 The number of requests received during 2017/18 are detailed in Table 10 below and compared to 2016/17 increased by 5% overall.

Table 10 – NAFN Requests Received

Type of Request	2017/18	2016/17	2015/16
General Data Protection Requests	38,980	47,765	62,703
Social Security Fraud Act	-	-	11,219
Driver and Vehicle Licensing Agency	16,507	15,489	14,478
Regulation of Investigatory Powers Act	760	946	1,035
Prevention of Social Housing Fraud Act/Council Tax Reduction Scheme	12,425	8,449	6,802
Sub Total	68,672	72,649	96,237
Type B (Online)	112,341	99,227	80,980
Grand Total	181,013	171,876	177,217
% Increase/(Decrease)	5%	(3%)	(13%)

- 6.8 The number and type of requests received is reported quarterly to the Executive Board and progress is monitored closely to ensure that staffing levels are appropriate to ensure requests are processed in line with performance standards and that other key services linked to the marketing strategy are delivered.

7 RISK MANAGEMENT AND INSURANCE

7.1 The approved priorities for 2017/2018 were:-

- To review the risk management system to ensure that it complies with best practice but is still practical for use by the organisation;
- To facilitate the delivery of risk workshops to enable both the Corporate Risk Register to be updated and Operational Risk Registers to be maintained by managers;
- To facilitate the continued implementation of the Information Governance Framework and prepare for the introduction of the General Data Protection Regulations which become effective from May 2018;
- To review the Business Continuity Management system in place to streamline the process to create a management tool that is workable, with the capability to provide knowledge and information should a major incident occur affecting service delivery; and
- To continue to support managers to assess their risks as services are redesigned to ensure that changes to systems and procedures remain robust and resilient offering cost effective mitigation and that claims for compensation can be successfully repudiated and defended should litigation occur.

7.2 Progress to review the risk management process has been delayed due to capacity issues and conflicting priorities.

7.3 Work has focused on the information governance agenda in light of the introduction of the General Data Protection Regulations (GDPR), which will become effective in May 2018 together with the new Data Protection Act. Work has concentrated on:

- Reviewing our policies and procedures to identify which need to be updated;
- Working with the Information Champions Group to raise their awareness of the changes introduced by GDPR and the new Data Protection Act;
- Undertaking Information Asset Audits across the Council, so that a Register of Processing Activities can be produced and the information collated can be used to update our privacy notices.
- An Information Governance newsletter has been introduced.

7.4 The team was restructured in February 2018 and the final stage of the recruitment process is underway to appoint the second Risk, Insurance and Information Officer.

7.5 The Insurance Renewal process, which is undertaken annually in March, was completed successfully and the Council is now in the final two years of its long-term agreement with its insurance providers. Continued support in relation to insurance claims has been provided to both service areas and schools throughout the year to ensure that claims against the Council are robustly defended.

8 PERFORMANCE INDICATORS

8.1 The performance of the section is monitored in a variety of ways and a number of indicators have been devised to enable comparisons between financial years and between similar organisations. Formal benchmarking using the Chartered Institute of Public Finance and Accountancy has not taken place for a number of years due to budget cuts and capacity; however, this is being reviewed by the North West Chief Audit Executive Group to determine if a small number of key performance indicators could be compared locally.

8.2 The Key Performance Indicators for Internal Audit for 2017/18 are detailed in Table 11 below and they are compared to the two previous years 2016/17 and 2015/16. All five performance indicators have been achieved.

Table 11 - Key Performance Indicators 2017/18

	INDICATOR	TARGET	17/18	16/17	15/16	Comments
1	Compliance with Public Sector Internal Audit Standards	100%	100%	100%	100%	Target Achieved
2	% of Plan Completed	93%	93%	93%	94%	Target Achieved
3	Customer Satisfaction (per questionnaires)	90% of customers "satisfied \geq 65%"	100%	94%	95%	Target Achieved
4	% Recommendations Implemented	90%	90%	92%	92%	Target Achieved
5	No. of Irregularities Reported/Investigated	Downward Trend	8	15	14	Target Achieved

- 8.3 Whilst all five targets have been achieved, it must to be acknowledged that not all the measures used are fully within the control of the team as explained below.
- 8.4 With regards to the Percentage of Plan Complete this a volatile indicator and affected by the timing of audits, staff availability in both internal audit and services areas to support the audit, reactive work (irregularities) and the timing of in year priority requests.
- 8.5 The Percentage of Recommendations Implemented indicator whilst demonstrating that the standard and quality of recommendations made are acceptable, their implementation is the responsibility of management and delays can occur for example due to lack of capacity, new systems and service redesigns.
- 8.6 The number of Irregularities Reported/investigated has decreased from fifteen to eight, however, this is a reactive indicator and not within the team's control.
- 8.7 The effectiveness of the team in terms of adding value to the Council is an important element of the role of internal audit (as per the definition outlined in section 1.1) and the service as a whole, however, it is extremely difficult to use quantitative indicators to measure this performance. Added value is demonstrated by the variety of work undertaken above, the responsive and flexible approach adopted, the positive comments and feedback received from auditees and the opinion of our External Auditors that they can place reliance on the work of Internal Audit.

9. QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME (QAIP)

- 9.1 The process and procedures in place within Internal Audit are continually reviewed and any issues/inefficiencies identified are addressed immediately to assist and improve productivity.
- 9.2 The Audit Management System 'Galileo' has been upgraded to the latest version available, however, the planned improvements to review the process for conducting post audit reviews, improving the indexing system and enhancing the reporting function have been rescheduled to 2018/19 due to capacity issues.
- 9.3 Work across the team was undertaken in preparation for the Peer Review, which was undertaken in March 2018 to assess compliance with the Public Sector Internal Audit

Standards (PSIAS). As reported earlier on the Agenda, the service was judged to be compliant with the standards and the recommendations made have been included in the Quality and Assurance Improvement Programme for 2018/19 which will be presented to the Audit Panel as part of the Risk Management and Audit Service Plan for 2018/19 Report later on the agenda.

10 INDEPENDENCE OF INTERNAL AUDIT

- 10.1 In accordance with the Public Sector Internal Audit Standards, the Internal Audit Team/Function has continued to remain independent of any non-audit operational responsibilities during 2017/18.
- 10.2 In the Peer Review Report dated 3 May 2018 a recommendation was included regarding the role of the Head of Risk Management and Audit as stated below. A meeting has been arranged with the Director of Governance and Pensions and the Director of Finance to discuss this recommendation.

“Standard - 1130 Impairment to Independence or Objectivity

A management decision was taken to give the Head of Risk Management and Audit the role of the Senior Information Risk Owner (SIRO). As the nominated SIRO the Head of Risk Management and Audit owns information governance risks for the Council which impairs the independence required to provide assurance of this function”.

11 AUDIT OPINION BASED ON RESULTS OF 2017/18 ACTIVITY

- 11.1 The Audit Panel can take reasonable assurance that arrangements to secure governance, risk management and internal control, within those areas reviewed, are suitably designed and applied effectively.
- 11.2 It has to be accepted that the gross risk for the Council has increased in recent years (as we have reduced capacity whilst still having to deliver a significant change programme to meet our financial challenges). The finding of our work is that controls are in place to mitigate these risks and where improvements have been highlighted, managers have agreed to implement the suggested recommendations. This will aid the management of risks and support the overall control environment.

12 RECOMMENDATION

- 12.1 Members note the report and the performance of the Risk Management and Audit Service during 2017/18.

Activity Title	Purpose of Audit	Approved Plan	Revised Plan	Actual Days	Variance	Status	Level of Assurance
ADULTS							
Home Care	To provide assurance that effective internal controls are in place in respect of the provision of homecare.	15	0	0	0	Reablement was identified as a priority	
Reablement	To provide assurance that effective internal controls are in place in respect of the reablement service.	0	15	20	5	Final Report Issued	Medium Level of Assurance
Learning Disabilities Client Accounts	To provide assurance that effective internal controls are in place to ensure that clients monies are safeguarded and appropriately accounted for.	10	10	17	7	Final Report Issued	Medium Level of Assurance
PAR - Planning and Commissioning - Strategic Management	Follow up work to ensure audit recommendations have been implemented.	3	3	3	0	Completed	
PAR - Nursing and Residential Home Placements-Payments	Follow up work to ensure audit recommendations have been implemented.	1	1	0	-1	Suspended	
PAR - Community Response and Telecare-Telehealth	Follow up work to ensure audit recommendations have been implemented.	3	3	4	1	Completed	
Control Report - Missing Monies - Somerset House Learning Disabilities Home	As a result of monies going missing at a Learning Disabilities Home a Control Report was produced. The Control Report identified weaknesses in processes and made recommendations which, once implemented, will strengthen the control environment and reduce the risk of such an incident occurring in the future.	1	1	1	0	Completed	
Planning and Control - Adult Services		8	8	8	0	Completed	
Advice - Adult Services		9	9	10	1	Completed	
Post Audit Reviews		9	9	0	-9	Days Reallocated	
	Totals	59	59	62	3		
CHILDREN'S							
Childrens Services Reporting of Performance Data to the Improvement Board	Days allocated to review the performance data provide to the Improvement Board for accuracy and completeness.	15	15	7	-8	Performance Management has now transferred to the Policy, Performance and Communications Team.	
Safeguarding	This review will examine the risks and the controls in place to mitigate those risks, in relation to Safeguarding Children.	15	15	19	4	Draft Report Issued	
Childrens Homes	The financial procedures at the Homes will be reviewed.	20	0	0	0	Rescheduled to 2018/19	

Placements North West	Placements Northwest is a regional children's service project which assists the 22 local authorities in the Northwest in making "Out of Authority" placements. These placements cover four board areas: Education, Fostering, Leaving Care and Residential sectors. Tameside is the lead authority for the project. This audit follows on from an audit on the Procurement of Placements which was conducted in 2015/16. We will review the processes in place for the award of contracts/frameworks that have been set up, and also the monitoring of the contracts/frameworks.	15	0	0	0	Service transferred to another GM Authority and responsibility for the audit has also transferred.	
Leaving Care	To provide assurance that internal controls are in place to ensure effective transition from the leaving care service.	15	15	25	10	Draft Report Issued	
Emergency/Cash Payments	To provide assurance that internal controls are in place to ensure effective transition from the leaving care service.	10	10	0	-10	Rescheduled to 2018/19	
PAR - Procurement of Placements for Children	Follow up work to ensure audit recommendations have been implemented.	0	3	3	0	Work in Progress	
PAR - ISCAN Short Term Care - Jubilee Gardens	Follow up work to ensure audit recommendations have been implemented.	1	1	0	-1	Completed	
Advice - Tapestry Sign Off	To ensure appropriate controls are in place prior to signing the system off.	0	0	2	2	Work in Progress	
Control Report - Information Incidents	To comment on control issues highlighted as a result of information incidents.	0	0	2	2	Work in Progress	
Troubled Families	To provide assurance that internal controls are in place to ensure effective transition from the leaving care service.	10	10	15	5	Final Report Issued	Medium Level of Assurance
Planning and Control		6	6	4	-2	Completed	
Post Audit Reviews		6	3	0	-3	Days Reallocated	
Advice		5	6	0	-6	Completed	
Totals		117	84	76	-8		

POPULATION HEALTH

Public Health - Contract Monitoring - Provision of a Drug and Alcohol Recovery Service	To review the process in place for monitoring the Drugs and Alcohol contract to ensure that it is robust and achieving the required outcomes	2	2	2	0	Final Report Issued	Low Level of Assurance
Health and Wellbeing - Health Visiting Service	To review the process in place for the commissioning and monitoring of the Health Visiting Service as an aspect of the mandatory Healthy Child Programme (0-5)	15	15	0	-15	Rescheduled to 2018/19	
Ring-fenced Public Health Grant	Certification to confirm that expenditure has been incurred in accordance with the grant conditions.	5	5	6	1	Completed	

PAR - Public Health - Contract Monitoring - Provision of a Drug and Alcohol Recovery Service	Follow up work to ensure audit recommendations have been implemented.	2	2	4	2	Work in Progress	
Post Audit Review - Information Governance	Follow up work to ensure audit recommendations have been implemented.	1	1	1	0	Completed	
Planning and Control		3	3	3	0	Completed	
Advice		1	1	0	-1	Completed	
	Totals	29	29	16	-13		
PLACE							
Section 106 Agreements, Developer Levy and Community Infrastructure Levy	To provide assurance that effective internal controls are in place in respect of the provision of Section 106 Agreements.	1	1	2	1	Final Report Issued	Low Level of Assurance
Hattersley Collaboration Agreement	To undertake an audit of the Final Accounts.	1	1	2	1	Completed	
Hattersley Collaboration Agreement	To undertake an audit of the Final Accounts.	6	6	9	3	Completed	
Estate Management	To provide assurance that the Council's Estate is being effectively managed and income is being maximised.	15	15	15	0	Draft Report Issued	
Capital Projects	To examine the project management process in respect of a number of major capital schemes to provide assurance that it is operating effectively and achieving the required outcomes.	15	0	0	0	Deferred	
Post Audit Review - Inspired Spaced - Monitoring of the Facilities Management Contract	Follow up work to ensure audit recommendations have been implemented.	0	0	7	7	Work in Progress	
Inspired Spaces - Monitoring Of The Catering Contract	To provide assurance that effective contract monitoring processes are in place in order to ensure compliance.	15	0	0	0	Suspended	
Post Audit Review- Section 106 Agreements, Developer Levy and Community Infrastructure Levy	Follow up work to ensure audit recommendations have been implemented.	3	3	0	-3	Work in Progress	
Planning and Control		4	4	4	0	Completed	
Advice and Support		2	2	1	-1	Completed	
Post Audit Reviews		0	0	0	0	Days Reallocated	
	Totals	62	32	39	3		
OPERATIONS AND NEIGHBOURHOODS							
Use Of CCTV	To provide assurance that effective internal controls are in place in respect of the provision of the Closed Circuit Television system.	15	15	23	8	Draft Report Issued	
Health and Safety Consultancy Review	To provide assurance that health and safety is being effectively managed throughout the Council and ensure compliance with legislation.	3	3	3	0	Consultancy Report Issued.	
Audit of Final Accounts	To provide assurance that the figures contained within the final accounts are correct.	5	0	0	0	Deferred	

Environmental Services Income	To review the process in place for the collection of environmental services income to ensure that it is maximised, promptly collected and appropriately accounted for.	15	0	0	0	Deferred	
Waste Disposal Levy	To provide assurance that effective internal controls are in place to ensure that the waste disposal levy has been correctly determined.	15	0	1	1	Suspended	
Provision of the Integrated Transport Service	To provide assurance that effective internal controls are in place to ensure that the waste disposal levy has been correctly determined.	15	15	5	-10	Work in Progress	
Local Authority Bus Subsidy Grant	To provide assurance that effective internal controls are in place to ensure that the waste disposal levy has been correctly determined.	1	1	2	1	Completed	
PAR - Stores and Stock Control	Follow up work to ensure audit recommendations have been implemented.	1	1	1	0	Completed	
PAR - Markets Operations		2	2	1	0	Completed	
PAR - Car Parking and Enforcement Income		2	4	4	0	Completed	
Planning and Control		7	7	7	0	Completed	
Advice		12	12	9	-3	Completed	
Post Audit Reviews		6	5	0	-5	Days Reallocated	
Totals		98	64	54	-9		

GOVERNANCE

NNDR Full System	To examine the internal controls in place regarding the collection of NNDR income to ensure it is maximised, promptly recovered and correctly accounted for.	15	15	20	5	Work in Progress	
Determination and Recovery Of Charges	To review the processes in place within Exchequer Services to ensure that charges are being correctly calculated and promptly recovered.	15	0	0	0	Rescheduled to 2018/19	
Council Tax Full System	To examine the internal controls in place regarding the collection of Council Tax income to ensure it is promptly collected, maximised and correctly accounted for.	15	15	16	1	Draft Report Issued	
Debtors	To provide assurance that all invoices are correctly raised and income is promptly collected and appropriately accounted for.	10	0	0	0	Rescheduled to 2018/19	
PAR - Direct Payments	Follow up work to ensure audit recommendations have been implemented.	3	6	3	-3	Work in Progress	
UK Mail - System Sign Off	Transfer of system to UK Mail. Internal Audit will carry out check to sign it off prior to going live.	5	5	15	10	Work in Progress	
Planning and Control		6	6	5	-1	Completed	
Advice		10	10	15	5	Completed	
Post Audit Reviews		4	1	0	-1	Days Reallocated	

Payroll Whole System	To review the controls in place for the payment of salaries, additional payments, and the deduction of tax, other statutory deductions and pension contributions.	7	7	10	3	Final Report Issued	High Level of Assurance
DBS Procedures	Review of the processes in operation across the Council, to see if the appropriate controls are in place, and whether there are any improvements that can be made.	3	3	3	0	Final Report Issued	Medium Level of Assurance
Payroll - External Audit Checks	Grant Thornton select a sample from iTrent and Internal Audit carry out checks and provide the evidence to support the transactions. External Audit rely on this work to obtain assurance that the payroll system is operating effectively.	5	5	0	-5	Audit not required in 2017/18	
Softbox	A review is planned to look at the whole system from Childrens Services through to the payment on Softbox, to ensure that the controls to prevent overpayments are operating effectively.	15	0	0	0	Rescheduled to 2018/19	
Creditors Full System	To provide assurance that all invoices and payment requisitions are paid correctly, on a timely basis, and expenditure is appropriately accounted for.	15	15	21	6	Draft Report Issued	Low Level of Assurance
Registrars	An allocation is included in the Plan each year to review the records and income in respect of individual Registrars, on cyclical basis.	6	6	5	-1	Draft Report Issued	
Members Allowances - Publication	To provide data assurance in relation to the publication of members allowances.	2	2	3	1	Completed	
Car Allowances Annual Review	To undertake checks on the annual review of Car Allowances for correctness.	0	0	1	1	Completed	
Post Audit Review - Creditors	Follow up work to ensure audit recommendations have been implemented.	0	1	1	0	Incorporated into the Audit	
PAR Payroll Whole System	Follow up work to ensure audit recommendations have been implemented.	2	2	1	-1	Work In Progress	
GMPF Annual Return - Compliance Checks	Checks on the compliance checklist submitted with the GMPF Annual Return, to enable it to be signed off by the Head of Internal Audit.	3	3	4	1	Completed	
Control Report - Information Incidents	To comment on control issues highlighted as a result of Information Incidents	0	0	3	3	Completed	
Agresso Upgrade	Signing off the upgrade of the General Ledger system.	0	0	2	2	Work in Progress	
Planning and Control		6	6	1	-5	Completed	
Advice and Support		3	3	24	21	Completed	
Post Audit Reviews		8	6	0	-6	Days Reallocated	
Totals		156	117	151	34		

FINANCE							
External Audit Checks - General Expenditure	To undertake checks on a sample of expenditure transactions to ensure that they are appropriate to the needs of the Council, have been appropriately authorised and correctly accounted for. This task is undertaken on behalf of External Audit and the results are used to inform the Audit of the Final Accounts.	5	5	11	6	Completed	
Review of Financial Regulations	To review and make recommendations to update Financial Regulations.	1	1	0	-1	Work In Progress	
VAT	To provide assurance that VAT is being appropriately accounted for.	10	10	12	2	Draft Report Issued	
Monitoring of Capital Programme	To provide assurance that effective monitoring arrangements are in place in respect of capital expenditure.	2	2	4	2	Final Report Issued	Medium Level of Assurance
Treasury Management	To provide assurance that effective internal controls are in place in respect of the provision of the Treasury Management function.	15	15	13	-2	Draft Report Issued	
PAR - Better Care Fund	Follow up work to ensure audit recommendations have been implemented.	1	3	3	0	Work in Progress	
PAR - Cashiers		2	3	3	0	Completed	
PAR - Review of Financial Systems - General Ledger and Budgetary Control		0	5	5	0	Completed	
Planning and Control		5	5	4	-1	Completed	
Advice and Support		12	12	4	-8	Completed	
Post Audit Reviews		9	1	0	-1	Days Reallocated	
Network Security (incl 3rd Party access)	This audit, to be carried out by Salford ICT Audit team, will examine the management of the network and the security measures in place, to safeguard the Authority's information assets.	10	0	0	0	Rescheduled to 2018/19	
BACS - New System Sign Off	New BACS software is to be introduced and Internal Audit will carry out checks to sign it off prior to it going live.	3	3	3	0	Work in Progress	
Device Management	To provide assurance that effective internal controls are in place in respect of Device Management.	3	3	7	4	Final Report Issued	Medium Level of Assurance
Computer Audit Contingency	This is an allocation of days to enable us to draw on the expertise of the ICT Auditors at Salford for advice and assistance with other audits.	5	5	0	-5	Days to be allocated to support other audits where ICT advice/support needed	
Audit Needs Assessment	To undertake a risk assessment to determine the ICT Audits for future planning years	3	3	0	-3	Work in Progress	
PAR Device Management	Follow up work to ensure audit recommendations have been implemented.	0	3	3	0	Completed	
Planning and Control		4	4	0	-4	Completed	
Advice and Support		7	7	2	-5	Completed	
Post Audit Reviews		3	0	0	0	Days Reallocated	
Totals		100	89	73	-16		

LEARNING							
Poplar St Primary Nursery	To review the financial management of the school to ensure robust processes and procedures are in place in accordance with best practice to deliver a strong control environment.	6	6	6	0	Final Report Issued	High Level of Assurance
Holden Clough Primary and Nursery		0	0	4		Draft Report Issued	
Arlies Primary and Nursery		6	6	6	0	Final Report Issued	High Level of Assurance
Millbrook Prim and Nursery		6	6	6	0	Final Report Issued	High Level of Assurance
Aldwyn Primary		6	6	7	1	Final Report Issued	Medium Level of Assurance
St. Anne's Primary, Denton		6	6	6	-1	Work In Progress	
Dane Bank Primary and Nursery		0	0	7	7	Final Report Issued	Medium Level of Assurance
St Pauls R C Primary and Nursery Hyde		6	6	6	0	Final Report Issued	High Level of Assurance
Ravensfield Primary		6	6	0	-6	Rescheduled to 2018/19	
Holy Trinity C E Gee Cross		6	6	3	-3	Work In Progress	
St Johns C E Primary		6	6	0	-6	Rescheduled to 2018/19	
St Marys R C Primary Denton		6	6	6	0	Final Report Issued	High Level of Assurance
Holy Trinity C E Primary		6	6	0	-6	Rescheduled to 2018/19	
St Marys C E Infant and Nursery Droylsden		6	6	0	-6	Rescheduled to 2018/19	
St Marys R C Primary and Nursery, Dukinfield		6	6	7	1	Draft Report Issued	
St Anne's R C Primary and Nursery, Audenshaw		6	6	9	3	Draft Report Issued	
Samuel Laycock School		6	6	0	-6	Rescheduled to 2018/19	
St. Georges C E Primary Mossley		6	6	7	1	Final Report Issued	Medium Level of Assurance
Alders Community High School		10	10	12	2	Final Report Issued	Medium Level of Assurance
Thomas Ashton Primary and Secondary Centres		10	10	9	-1	Work in Progress	
St Raphael's R C Primary		2	2	1	-1	Final Report Issued	Medium Level of Assurance
Canon Burrows C E Primary		2	2	4	2	Final Report Issued	Low Level of Assurance
Livingstone Primary		1	1	2	1	Final Report Issued	High Level of Assurance
Hyde Community College		1	1	3	2	Final Report Issued	Low Level of Assurance
Milton St Johns C E Primary		1	1	2	1	Final Report Issued	High Level of Assurance
St Peters RC Primary and Nursery Stalybridge		1	1	2	1	Final Report Issued	High Level of Assurance
St Stephens R C Primary Droylsden - ICT Consultancy Review	To provide assurance on the ICT provision with the school	0	0	5	5	Review Completed	
Wild Bank Primary and Nursery - Control Report	To improve the controls in the school	0	0	7	7	Review Completed	
PAR - Music Service Control Report	Follow up work to ensure audit recommendations have been implemented	0	0	3	3	Completed	
ICT Security at Schools	Salford ICT Auditors will review the systems and processes in place at a sample of schools for ICT Security and Information Governance. Good practice and recommendations will be shared.	20	20	11	-9	Final Report Issued	Low Level of Assurance
Schools Cash Flow/Deficit Recovery Plans	Review of the procedures for monitoring the cash deficits at schools and the risks to the Council with the Academisation programme.	1	1	3	2	Final Report Issued	Medium Level of Assurance
Pupil Referral Service	Review of the controls in place to mitigate the risks within the Pupil referral Service.	2	2	3	1	Final Report Issued	Low Level of Assurance

Planning and Control		9	9	4	-5	Completed	
Advice		15	15	8	-7	Completed	
Schools Newsletter		0	0	2	2	Completed	
Post Audit Reviews		6	0	0	0	Days Reallocated	
Mossley Hollins High Grant Claim - Assurance Work		2	2	3	1	Completed	
PAR - Russell Scott Primary	Follow up work to ensure audit recommendations have been implemented.	2	2	3	1	Work In Progress	
PAR - Denton Community College		2	2	2	0	Completed	
PAR - Pinfold Primary and Nursery		1	1	1	0	Completed	
PAR - Canon Johnson C E Primary		1	1	1	0	Completed	
PAR - Hurst Knoll C E Primary		1	1	1	0	Completed	
PAR - Greenfield Primary and Nursery		1	1	1	0	Completed	
PAR - St James R C Primary and Nursery Hattersley Hyde		1	1	1	0	Completed	
PAR - Early Years Funding		3	3	4	1	Completed	
PAR - Greswell Primary and Nursery		2	2	1	-1	Completed	
PAR - Our Lady Of Mount Carmel		3	3	3	0	Completed	
PAR - Milton St Johns C E Primary		1	1	0	-1	Work In Progress	
PAR - Canon Burrows C E Primary		1	1	2	1	Completed	
PAR - St Raphael's			1	1	0	Completed	
PAR - Arlies Primary and Nursery			1	0	-1	Work In Progress	
PAR - Control Report - Wildbank Primary and Nursery		1	2	2	0	Completed	
PAR - Millbrook Primary and Nursery			1	0	-1	Work In Progress	
PAR - Poplar St Primary and Nursery			1	0	-1	Work In Progress	
PAR - Livingstone Primary		1	1	1	0	Completed	
PAR - St Pauls RC Primary and Nursery				0		Work In Progress	
PAR - St Peters RC Primary and Nursery Stalybridge		1	1	1	0	Work In Progress	
PAR - Hyde Community College		2	2	0	-2	Work In Progress	
PAR - Pupil Referral Service		3	3	2	-1	Work In Progress	
PAR - School Cash Flow/Deficit Recovery Plans		0	0	0	0	Rescheduled to 2018/19	
	Totals	205	205	189	-21		
CROSSCUTTING							
Integrated Commissioning Fund	To provide assurance that effective internal controls are in place for the effective financial management and budgetary control of the Integrated Commissioning Fund.	15	0	0	0	Deferred	
Contingency for Greater Manchester Combined Authority/Devolution Assurance and Joint Working	Work programme to be determined by the Greater Manchester Audit Executive Group.	20	20	6	-14	Completed all Grant Assurance Work	

Information Governance - Mobile Working	With the increase in mobile working, this review will aim to assess whether there are appropriate controls in place to keep information secure.	15	0	0	0	Will be covered as part of the Information Governance Audit in the 2018/19 Plan	
Planning and Control		1	1	0	-1	Completed	
Post Audit Reviews		2	2	0	-2	Days Reallocated	
Totals		53	23	6	-17		



GREATER MANCHESTER PENSION FUND

Contribution Income (including processing of Year End Returns)	Contribution Income is reviewed annually, as it is the main income of the Pension Fund, paid over to the Fund by Employers. External Audit rely on our work on this area, to ensure that there are processes in place to monitor and review the contributions received.	15	15	1	-14	Rescheduled to 2018/19	
Treasury Management	A review will be carried out alongside a review for Tameside on the Treasury Management system/process.	10	10	10	0	Work In Progress	
Benchmarking/KPI's	A review will take place of the Pension Fund's Benchmarks and Key Performance Indicators.	0	0	0	0	Rescheduled to 2018/19	
BACS	New BACS software is to be implemented, and when this is live a review will be carried out on the process followed by the Pension Fund when BACS payments are made, to ensure that internal controls are adequate.	3	3	3	0	Work In Progress	
First Bus Transfer to GMPF	Internal Audit will carry out some data verification checks on the transfer of the data from the ceding funds, into GMPF.	20	20	24	4	Completed	
First Bus Asset Transfers	To provide assurance that the asset transfer process to appropriately controlled.	5	5	0	-5	Rescheduled for 2018/19	
Private Equity	A review will be carried out on the system/process followed for the Private Equity Investments.	15	15	15	0	Final Report Issued	High Level of Assurance
Pooling of investments	An allocation has been included in the Plan to review the Governance arrangements in relation to Pooling.	0	0	0	0	Rescheduled to 2018/19	
Transfer of Assets to New Credit Manager	A new Credit Manager has been procured and assets will be moved from other Fund Managers to the new Credit Manager. Checks will be carried out on the completeness and accuracy of the transfer of assets.	5	5	11	6	Completed	
Local Investments Impact Portfolio	A review will be carried out on the system/process followed for the Local Investments Impact Portfolio.	15	15	19	4	Draft Report Issued	
Calculation and Payment of Benefits	Systems for the calculation of benefits will be examined, and followed through to the payment system.	15	15	8	-7	Work In Progress	

Guaranteed Minimum Pensions (GMP)	In April 2016, contracting out status for all UK Defined Benefit schemes, including the LGPS, ended. As a result, all schemes need to reconcile their GMP data against HMRC data to ensure liabilities are recorded correctly and to avoid overpayment of pensions. Audit time has been included in the Plan to review a sample of reconciliations and the process being followed.	5	5	8	3	Work In Progress	
Visits to Contributing Bodies	An allocation of days is included annually for Internal Audit to carry out visits to a sample of Employers. The auditor reviews the data held on the Employer's payroll system to ensure that the correct contributions are being paid over to the Pension Fund.	47	0	2	2	Days allocated as visits arranged.	
Visit to Contributing Body - Manchester City Council	To review the data held on the Employer's payroll system to ensure that the correct contributions are being paid over to the Pension Fund.	0	13	13	0	Draft Report Issued	
Visit to Contributing Body - Salford City Council		0	10	11	1	Draft Report Issued	
Visit to Contributing Body - Tameside MBC		0	14	16	2	Final Report Issued	High Level of Assurance
Visit to Contributing Body - Trafford MBC		0	10	9	-1	Work In Progress	
Contributing Body Visit to NPS		0	10	17	7	Final Report Issued	Low Level of Assurance
Payroll - Transfer to Java	To provide assurance that the transfer is managed effectively and data transfers are controlled/reconciled.	8	8	7	-2	Completed	
Agresso Upgrade	To sign off the Agresso upgrade prior to the system going live	10	10	7	-4	Work In Progress	
Altair Administration to Payroll Upgrade	To sign off the Altair Administration to Payroll upgrade prior to going live.	5	5	0	-5	Rescheduled to 2018/19	
ICT Device Management	To provide assurance that effective internal controls are in place in respect of Device Management.	10	10	11	1	Work In Progress	
Review of Compliance with TPR Code of Practice 14	To provide assurance that the Pension Fund is complying with the TPR Code of Practice 14.	10	10	5	-5	Work In Progress	
Advanced Contribution Scheme - Consultancy Advice	To provide advice that the controls in place are robust.	0	3	6	3	Completed	
Debtors	To provide assurance that all invoices are correctly raised and income is promptly collected and appropriately accounted for.	0	1	1	0	Final Report Issued	Medium Level of Assurance
VAT	To provide assurance that VAT is being appropriately accounted for.	0	9	13	4	Draft Report Issued	
Review of Fund Manager - Investec	A review will be carried out on the system/process followed by Investec.	0	8	10	2	Final Report Issued	High Level of Assurance
Review of the Management of Assets by La Salle Investment Manager	A review will be carried out on the system/process followed by La Salle Investment Manager.	0	1	1	0	Final Report Issued	High Level of Assurance

Greater Manchester Property Venture Fund	A review will be carried out on the system/process followed for the Greater Manchester Property Venture Fund.	0	15	27	12	Final Report Issued	Medium Level of Assurance
Pension Benefits Payable	Systems for the calculation of benefits will be examined, and followed through to the payment system.	0	1	2	0	Final Report Issued	High Level of Assurance
Employer Agreements Consultancy Advice		0	3	3	0	Completed	
Advice - Island Site Service Charge	Advice provided to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	0	0	2	2	Completed	
Advice - Service Charge Sign Off - Globe Park Rochdale		0	0	1	1	Completed	
Advice and Support - Reporting to the Local Board		0	0	4	4	Completed	
Advice and Support - Chorlton Cross Service Charge Sign Off		0	0	2	2	Completed	
Advice and Support - Employer Secure File Transfer		0	0	0	0	Completed	
Advice and Support - Audit Trail Deletion		0	0	0	0	Completed	
Advice and Support - Information Incidents	To assist management with the investigation into information incidents and provide advice on controls to prevent future occurrences.	0	0	1	1	Completed	
Altair	To review the controls in place within the system to ensure it is fit for purpose and robust.	0	5	5	0	Final Report Issued	High Level of Assurance
Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	2	0	0	0	Days Reallocated	
PAR - Debtors		1	1	0	-1	Work In Progress	
PAR - Private Equity			0	0		Work In Progress	
PAR - Review of the Management of Assets by La Salle Asset Management		1	1	1	0	Work In Progress	
PAR - Visits to Contributing Bodies - Police Authority		1	1	0	-1	Work In Progress	
PAR - Contributing Body Visit to NPS		0	0	12	12	Work In Progress	
PAR - Visits to Contributing Bodies - Manchester College		1	1	1	0	Work In Progress	
PAR - Review of Key Financial Systems - Creditors		1	1	1	0	Completed	
PAR - Visits to Contributing Bodies - New Charter Housing Trust		1	1	1	0	Completed	
PAR - Visit To Contributing Body - Rochdale Metropolitan Borough Council		1	0	0	0	Work In Progress	
PAR - Visits to Contributing Bodies - Manchester Airport		2	2	4	2	Completed	
PAR - Visits to Contributing Bodies - Stockport College		3	3	3	0	Completed	
PAR - Visit To Contributing Body - Bolton Borough Council		1	1	1	0	Work In Progress	
PAR - Pension Benefits Payable		1	1	0	-1	Work In Progress	

PAR - Visits to Contributing Bodies - Transport for Greater Manchester		1	1	1	0	Completed	
Planning and Control		15	15	15	0	Completed	
Advice and Support		20	17	6	-11	Completed	
Days to Complete 2016/17 Work		51	0	0	0	Days Reallocated	
NFI Data Matching		0		1	1	Completed	
	Totals	300	300	318	18		
FRAUD WORK/IRREGULARITY INVESTIGATIONS		487	487	501	52		
OVERALL TOTALS		1666	1489	1485	27		

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officer:	Kathy Roe – Director of Finance Wendy Poole – Head of Risk Management and Audit Services
Subject:	ANNUAL GOVERNANCE REPORT 2017/18
Report Summary:	<p>To present the Governance Report comprised of the two elements below for comment, challenge and approval:</p> <ol style="list-style-type: none">1. The Draft Annual Review against the Code of Corporate Governance for 2017/18 (Appendix 1).2. The Draft Annual Governance Statement for 2017/18 (Appendix 2).
Recommendations:	<p>That members approve the:</p> <ol style="list-style-type: none">1. Draft Annual Review against the Code of Corporate Governance for 2017/18.2. Draft Annual Governance Statement for 2017/18.
Links to Community Strategy:	Demonstrates proper Corporate Governance.
Policy Implications:	Demonstrates proper compliance with the Accounts and Audit Regulations 2015.
Financial Implications: (Authorised by the Section 151 Officer)	Sound corporate governance and proper systems of internal control are essential for the long-term financial health and reputation of the Council.
Legal Implications: (Authorised by the Borough Solicitor)	The production of the Annual Governance Statement meets the requirements of the Accounts and Audit Regulations 2015.
Risk Management:	The statement provides assurance that the Council has a sound system of corporate governance in place. It is considered to be an important public expression of how the Council directs and controls its functions and relates to its community.
Access to Information:	<p>The background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by:</p> <p> Telephone: 0161 342 3846</p> <p> e-mail: wendy.poole@tameside.gov.uk</p>

1 INTRODUCTION

- 1.1 Corporate Governance is the system by which the Council directs and controls its functions and relates to its community. This is the means by which sound and ethical practice can be assured and unacceptable practice identified and eradicated. Historically there has been a general recognition that all local authorities should be seen to meet the highest standards and governance arrangements possible.
- 1.2 The issues faced by local authorities in recent years reflecting social, economic, and legislative change have led to new, diverse ways of working as opposed to traditional roles. The common theme that continues to run through Government initiatives is the need for local authorities to review the various systems and processes they have in place for managing both their internal affairs and their relationships with their expanding number of key stakeholders. Together these systems comprise corporate governance.

2 CORPORATE GOVERNANCE REQUIREMENTS

- 2.1 The Framework Delivering Good Governance in Local Government, published by the Chartered Institute of Public Finance and Accountancy in association with Society of Local Authority Chief Executives in 2016, sets the standard for local authority governance in the UK. The Framework urges local authorities to review and report on the effectiveness of their governance arrangements.
- 2.2 The main principle underpinning the 2016 version of Delivering Good Governance in Local Government: Framework (2016) ('the Framework') continues to be that local government is developing and shaping its own approach to governance, taking account of the environment in which it now operates. The Framework is intended to assist authorities individually in reviewing and accounting for their own unique approach. The overall aim is to ensure that resources are directed in accordance with agreed policy and according to priorities, that there is sound and inclusive decision making and that there is clear accountability for the use of those resources in order to achieve desired outcomes for service users and communities.
- 2.3 The core principles of the Framework are: -
 - Behaving with integrity, demonstrating strong commitment to ethical standards and respecting the rule of law;
 - Ensuring openness and comprehensive stakeholder engagement;
 - Defining outcomes in terms of sustainable economic, social and environmental benefits;
 - Determining the intervention necessary to optimise the achievement of the intended outcomes;
 - Developing the entity's capacity including the capability of its leadership and the individuals within it;
 - Managing risks and performance through robust internal control and strong public financial management; and
 - Implementing good practices in transparency, reporting and audit to deliver effective accountability.
- 2.4 The Framework positions the attainment of sustainable economic, societal, and environmental outcomes as a key focus of governance processes and structures. Outcomes give the role of local government its meaning and importance, and it is fitting that they have this central role in the sector's governance. Furthermore, the focus on sustainability and the links between governance and public financial management are

crucial – local authorities must recognise the need to focus on the long term. Local authorities have responsibilities to more than their current electors as they must take account of the impact of current decisions and actions on future generations.

2.5 The Framework defines the principles that should underpin the governance of each local government organisation. It provides a structure to help individual authorities with their approach to governance. Whatever form of arrangements are in place, authorities should therefore test their governance structures and partnerships against the principles contained in the Framework by:

- reviewing existing governance arrangements;
- developing and maintaining an up-to-date local code of governance, including arrangements for ensuring ongoing effectiveness; and
- reporting publicly on compliance with their own code on an annual basis and on how they have monitored the effectiveness of their governance arrangements in the year and on planned changes.

3 ANNUAL REVIEW AGAINST THE CODE OF CORPORATE GOVERNANCE

3.1 A review has been completed assessing the Council's position against the approved Code of Corporate Governance in order to demonstrate compliance, ongoing developments/improvement and to prepare for the compilation of this year's Annual Governance Statement which is required, by the Accounts and Audit Regulations 2015.

3.2 The document was presented to the Single Leadership Team on 8 May 2018 for review and the draft Annual Review against the Code of Corporate Governance for 2017/18 incorporating all comments received is detailed at **Appendix 1**.

4 ANNUAL GOVERNANCE STATEMENT

4.1 The preparation and publication of an Annual Governance Statement is necessary to meet the requirements set out in Regulation 6 of the Accounts and Audit Regulations 2015. It requires authorities to "conduct a review at least once in a year of the effectiveness of its system of internal control" and "following the review, the body must approve an annual governance statement prepared in accordance with proper practices in relation to internal control".

4.2 The Draft Annual Governance Statement for 2017/18 which has been drawn up using the guidance contained within Delivering Good Governance in Local Government - Framework issued in 2016 is attached at **Appendix 2** for consultation and challenge.

4.3 The Annual Governance Statement is a corporate statement and covers both Tameside and the Greater Manchester Pension Fund.

4.4 The Annual Governance Statement is based on:-

- AGS Self-Assessment Checklists and signed Assurance Statements;
- Head of Risk Management and Audit's Annual Report;
- Medium Term Financial Plan/Budget Report;
- Review of System of Internal Audit;
- Annual Audit Letter;
- Role of the Chief Financial Officer;
- Role of the Head of Internal Audit;
- Corporate Plan; and

- Statutory Inspections.

- 4.5 This list is not exhaustive but it details the key elements of the assurance framework used to support the production of the Annual Governance Statement.
- 4.6 The format of the annual governance statement will be reviewed before the 2018/19 statement needs to be prepared to enable a comparison between the format used by the Council and the Tameside and Glossop Clinical Commissioning Group with the aim of introducing a format suitable for use across the Strategic Commission.
- 4.7 The Draft Annual Governance Statement 2017/18 has been presented to the Single Leadership Team and their comments have been incorporated into the document, together with those received from Policy, Performance and Communications.

5 CODE OF CORPORATE GOVERNANCE

- 5.1 The Code of Corporate Governance which complies with the Delivering Good Governance Framework of 2016 was approved in May 2016 for a three year period and no further updates are required.

6 EXECUTIVE CABINET

- 6.1 As in previous years this report will be circulated to the Executive Cabinet after the meeting by email for comments and any feedback will be incorporated into the documents.

7 EXTERNAL AUDIT

- 7.1 The Draft Annual Governance Statement will be signed off by the Director of Finance by 31 May for submissions to Grant Thornton (External Auditors) as it needs to accompany the Draft Statement of Accounts.
- 7.2 The final version incorporating any updates and comments from Grant Thornton will be presented to the Overview (Audit) Panel on 30 July for approval. It will then be signed by the Executive Leader and the Chief Executive and presented formally to Grant Thornton. Until this date the Annual Governance Statement is a live document and needs to be updated for any issues that come to light affecting the governance arrangements in place.

8 RECOMMENDATIONS

- 8.1 That members approve the:-
 - Draft Annual Review against the Code of Corporate Governance for 2017/18.
 - Draft Annual Governance Statement for 2017/18.

DRAFT REVIEW AGAINST THE
CODE OF CORPORATE
GOVERNANCE
2017-18

Introduction

The main principle underpinning the development of the new Delivering Good Governance in Local Government: Framework (CIPFA/Solace, 2016) ('the Framework') continues to be that local government is developing and shaping its own approach to governance, taking account of the environment in which it now operates. The framework is intended to assist authorities individually in reviewing and accounting for their own unique approach. The overall aim is to ensure that resources are directed in accordance with agreed policy and according to priorities, that there is sound and inclusive decision making and that there is clear accountability for the use of those resources in order to achieve desired outcomes for service users and communities.

The Framework positions the attainment of sustainable economic, societal, and environmental outcomes as a key focus of governance processes and structures. Outcomes give the role of local government its meaning and importance, and it is fitting that they have this central role in the sector's governance. Furthermore, the focus on sustainability and the links between governance and public financial management are crucial – local authorities must recognise the need to focus on the long term. Local authorities have responsibilities to more than their current electors as they must take account of the impact of current decisions and actions on future generations.

The Framework defines the principles that should underpin the governance of each local government organisation. It provides a structure to help Individual authorities with their approach to governance. Whatever form of arrangements are in place, authorities should therefore test their governance structures and partnerships against the principles contained in the Framework by:

- reviewing existing governance arrangements
- developing and maintaining an up-to-date local code of governance, including arrangements for ensuring ongoing effectiveness
- reporting publicly on compliance with their own code on an annual basis and on how they have monitored the effectiveness of their governance arrangements in the year and on planned changes.

The term 'local code' essentially refers to the governance structure in place as there is an expectation that a formally set out local structure should exist, although in practice it may consist of a number of local codes or documents.

To achieve good governance, each local authority should be able to demonstrate that its governance structures comply with the core and sub-principles contained in this Framework. It should therefore develop and maintain a local code of governance/governance arrangements reflecting the principles set out.

It is also crucial that the Framework is applied in a way that demonstrates the spirit and ethos of good governance which cannot be achieved by rules and procedures alone. Shared values that are integrated into the culture of an organisation, and are reflected in behaviour and policy, are hallmarks of good governance.

Principles of Good Governance

Principle A - Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.

Local government organisations are accountable not only for how much they spend, but also for how they use the resources under their stewardship. This includes accountability for outputs, both positive and negative, and for the outcomes they have achieved. In addition, they have an overarching responsibility to serve the public interest in adhering to the requirements of legislation and government policies. It is essential that, as a whole, they can demonstrate the appropriateness of all their actions and have mechanisms in place to encourage and enforce adherence to ethical values and to respect the rule of law.

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Key Evidence to Support Compliance	Additional Work Identified
Behaving with integrity	Ensuring members and officers behave with integrity and lead a culture where acting in the public interest is visibly and consistently demonstrated thereby protecting the reputation of the organisation.	<ul style="list-style-type: none"> • Member Code of Conduct • Officer Code of Conduct • Standards Committee • Induction • Annual Development Reviews 	
	Ensuring members take the lead in establishing specific standard operating principles or values for the organisation and its staff and that they are communicated and understood. These should build on the Seven Principles of Public Life (the Nolan Principles).	<ul style="list-style-type: none"> • Corporate Plan • Executive Leader's Annual Key Note Address • Constitution 	
	Leading by example and using these standard operating principles or values as a framework for decision making and other actions.	<ul style="list-style-type: none"> • Council Constitution – Article 17 Decision Making • Declaration of Interests at meetings • Standards Committee 	
	Demonstrating, communicating and embedding the standard operating	<ul style="list-style-type: none"> • Whistleblowing Policy • Anti-Fraud, Bribery and Corruption Strategy - 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Key Evidence to Support Compliance	Additional Work Identified
	principles or values through appropriate policies and processes which are reviewed on a regular basis to ensure that they are operating effectively.	Statement of Intent <ul style="list-style-type: none"> • Register of Gifts and Hospitality • Register of Interests • Complaints Policy • Codes of Conduct • Agendas/Minutes for Meetings 	
Demonstrating strong commitment to ethical values	Seeking to establish, monitor and maintain the organisation's ethical standards and performance.	<ul style="list-style-type: none"> • Scrutiny function • Standards Committee • Constitution - Decision Making 	
	Underpinning personal behaviour with ethical values and ensuring they permeate all aspects of the organisation's culture and operation.	<ul style="list-style-type: none"> • Chief Executive's Brief • The Wire • Team Briefings • Management Training – Strive Programme 	
	Developing and maintaining robust policies and procedures which place emphasis on agreed ethical values.	<ul style="list-style-type: none"> • Annual Development Review Process • Standards Committee • Recruitment Policies • Constitution 	
	Ensuring that external providers of services on behalf of the organisation are required to act with integrity and in compliance with high ethical standards expected by the organisation.	<ul style="list-style-type: none"> • Requirements built into contracts and agreements. 	
Respecting the rule of law	Ensuring members and staff demonstrate a strong commitment to the rule of the law as well as adhering to relevant laws and regulations.	<ul style="list-style-type: none"> • Constitution • Statutory Guidance • Qualified Officers in post • Circulation of Legal Updates 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Key Evidence to Support Compliance	Additional Work Identified
	Creating the conditions to ensure that the statutory officers, other key post holders and members are able to fulfil their responsibilities in accordance with legislative and regulatory requirements.	<ul style="list-style-type: none"> Statutory Officer roles Job Descriptions/Person Specifications Scheme of Delegation Compliance with CIPFA's Statement on the Role of the Chief Financial Officer in Local Government (CIPFA, 2015) 	
	Striving to optimise the use of the full powers available for the benefit of citizens, communities and other stakeholders.	<ul style="list-style-type: none"> Legal Implications are provided on all reports presented to Panels/Committees and Full Council. 	
	Dealing with breaches of legal and regulatory provisions effectively.	<ul style="list-style-type: none"> Monitoring Officer provisions Legal Implications provided Statutory provisions External/Internal Audit and Statutory Inspections 	
	Ensuring corruption and misuse of power are dealt with effectively.	<ul style="list-style-type: none"> Anti-Fraud, Bribery and Corruption policies and procedures Internal Audit Assurance 	

Principle B - Ensuring openness and comprehensive stakeholder engagement.

Local government is run for the public good; organisations therefore should ensure openness in their activities. Clear, trusted channels of communication and consultation should be used to engage effectively with all groups of stakeholders, such as individual citizens and service users, as well as institutional stakeholders.

Supporting-Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
Openness	Ensuring an open culture through demonstrating, documenting and communicating the organisation's commitment to openness.	<ul style="list-style-type: none"> • Council Website • Corporate Plan • Freedom of Information Act • Transparency Pages 	
	Making decisions that are open about actions, plans, resource use, forecasts, outputs and outcomes. The presumption is for openness. If that is not the case, a justification for the reasoning for keeping a decision confidential should be provided.	<ul style="list-style-type: none"> • Constitution – Article 17 Decision Making • Agendas/Minutes for Meetings are published on the Council's Website • Full Council Meetings are streamed on Social Media. 	
	Providing clear reasoning and evidence for decisions in both public records and explanations to stakeholders and being explicit about the criteria, rationale and considerations used. In due course, ensuring that the impact and consequences of those decisions are clear.	<ul style="list-style-type: none"> • Constitution – Article 17 Decision Making • Report Templates • Legal/Financial Implications provided on all reports provided to decision makers • Meeting date for Full Council, Panels and committees published on website • Constitution - Access To Information Procedure Rules • Agenda deadlines provided and adhered to • Safe and Sound Decision Making guidance 	
	Using formal and informal consultation and engagement to determine the most	<ul style="list-style-type: none"> • Corporate Plan • Consultation – Big Conversation 	

Supporting-Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	appropriate and effective interventions/courses of action.	<ul style="list-style-type: none"> Partnership Engagement Network Town Councils 	
Engaging comprehensively with institutional stakeholders	Effectively engaging with institutional stakeholders to ensure that the purpose, objectives and intended outcomes for each stakeholder relationship are clear so that outcomes are achieved successfully and sustainably.	<ul style="list-style-type: none"> Communication Strategy Service Area Plans Corporate Plan Partnership Engagement Network 	
	Developing formal and informal partnerships to allow for resources to be used more efficiently and outcomes achieved more effectively	<ul style="list-style-type: none"> Specific Partnership Agreements Budget Report Partnership Engagement Network 	
	Ensuring that partnerships are based on: <ul style="list-style-type: none"> Trust a shared commitment to change a culture that promotes and accepts challenge among partners and that the added value of partnership working is explicit. 	<ul style="list-style-type: none"> Partnership Agreements 	
Engaging with individual citizens and service users Effectively.	Establishing a clear policy on the type of issues that the organisation will meaningfully consult with or involve individual citizens, service users and other stakeholders to ensure that service (or other) provision is contributing towards the achievement of	<ul style="list-style-type: none"> Consultation – Big Conversation Town Councils Specific Partnership Agreements Partnership Engagement Network 	

Supporting-Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	intended outcomes.		
	Ensuring that communication methods are effective and that members and officers are clear about their roles with regard to community engagement.	<ul style="list-style-type: none"> Communications strategy 	
	Encouraging, collecting and evaluating the views and experiences of communities, citizens, service users and organisations of different backgrounds including reference to future needs.	<ul style="list-style-type: none"> Communications Strategy Joint Strategic Needs Assessment Partnership Engagement Network 	
	Implementing effective feedback mechanisms in order to demonstrate how their views have been taken into account.	<ul style="list-style-type: none"> Communication Strategy Complaints Procedure Citizen Magazine 	
	Balancing feedback from more active stakeholder groups with other stakeholder groups to ensure inclusivity	<ul style="list-style-type: none"> Consultation AGMA Meetings Council/Health Meetings 	
	Taking account of the interests of future generations of tax payers and service users.	<ul style="list-style-type: none"> Corporate Plan Service Plans Joint Strategic Needs Assessment 	

Principle C - Defining outcomes in terms of sustainable economic, social, and environmental benefits.

The long-term nature and impact of many of local government's responsibilities mean that it should define and plan outcomes and that these should be sustainable. Decisions should further the authority's purpose, contribute to intended benefits and outcomes, and remain within the limits of authority and resources. Input from all groups of stakeholders, including citizens, service users, and institutional stakeholders, is vital to the success of this process and in balancing competing demands when determining priorities for the finite resources available.

Supporting-Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
Defining outcomes	Having a clear vision which is an agreed formal statement of the organisation's purpose and intended outcomes containing appropriate performance indicators, which provides the basis for the organisation's overall strategy, planning and other decisions.	<ul style="list-style-type: none"> Corporate Plan Executive Leader's Annual Key Note Address 	
	Specifying the intended impact on, or changes for, stakeholders including citizens and service users. It could be immediately or over the course of a year or longer.	<ul style="list-style-type: none"> Corporate Plan Community Engagement Service Plans Town Councils 	
	Delivering defined outcomes on a sustainable basis within the resources that will be available.	<ul style="list-style-type: none"> Medium Term Financial Strategy Annual Budget Report Monitoring Reports 	
	Identifying and managing risks to the achievement of outcomes.	<ul style="list-style-type: none"> Risk Management Policy and Strategy Performance Reports Risk Management Comments on all reports to decision makers 	
	Managing service users expectations effectively with regard to determining	<ul style="list-style-type: none"> Corporate Plan Service Plans 	

Supporting-Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	priorities and making the best use of the resources available.	<ul style="list-style-type: none"> Executive Leaders Key Note Address Performance Indicators 	
Sustainable economic, social and environmental benefits	Considering and balancing the combined economic, social and environmental impact of policies, plans and decisions when taking decisions about service provision.	<ul style="list-style-type: none"> Legal/Financial Implications on all reports provided to decision makers Service Plans Medium Term Financial Plan Budget Report 	
	Taking a longer-term view with regard to decision making, taking account of risk and acting transparently where there are potential conflicts between the organisation's intended outcomes and short-term factors such as the political cycle or financial constraints.	<ul style="list-style-type: none"> Joint working Medium Term Financial Plan Consultation Decision Making reports/minutes are published on Website Forward Plan 	
	Determining the wider public interest associated with balancing conflicting interests between achieving the various economic, social and environmental benefits, through consultation where possible, in order to ensure appropriate trade-offs.	<ul style="list-style-type: none"> Consultation Constitution Article 17 - Decision making 	
	Ensuring fair access to services.	<ul style="list-style-type: none"> Corporate Equality Scheme Equality Impact Assessments 	

Principle D - Determining the interventions necessary to optimise the achievement of the intended outcomes.

Local government achieves its intended outcomes by providing a mixture of legal, regulatory, and practical interventions. Determining the right mix of these courses of action is a critically important strategic choice that local government has to make to ensure intended outcomes are achieved. They need robust decision-making mechanisms to ensure that their defined outcomes can be achieved in a way that provides the best trade-off between the various types of resource inputs while still enabling effective and efficient operations. Decisions made need to be reviewed continually to ensure that achievement of outcomes is optimised.

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
Determining interventions	Ensuring decision makers receive objective and rigorous analysis of a variety of options indicating how intended outcomes would be achieved and including the risks associated with those options. Therefore ensuring best value is achieved however services are provided.	<ul style="list-style-type: none"> • Constitution Article 17 – Decision making • Forward Plan • All reports to decision makers have legal/financial and risk management comments • External Audit – Value for Money Conclusion • Safe and Sound Decision Making Guidance 	
	Considering feedback from citizens and service users when making decisions about service improvements or where services are no longer required in order to prioritise competing demands within limited resources available including people, skills, land and assets and bearing in mind future impacts.	<ul style="list-style-type: none"> • Consultation Feedback • Medium Term Financial Plan • Complaints/Service Requests • Revenue/Capital Monitoring 	
Planning interventions	Establishing and implementing robust planning and control cycles that cover strategic and operational plans, priorities and targets.	<ul style="list-style-type: none"> • Meeting dates published • Forward Plan • Service planning process 	
	Engaging with internal and external	<ul style="list-style-type: none"> • Communication Strategy 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	stakeholders in determining how services and other courses of action should be planned and delivered.	<ul style="list-style-type: none"> Partnership Engagement Network 	
	Considering and monitoring risks facing each partner when working collaboratively including shared risks.	<ul style="list-style-type: none"> Specific Partnership Agreements Risk Registers 	
	Ensuring arrangements are flexible and agile so that the mechanisms for delivering outputs can be adapted to changing circumstances.	<ul style="list-style-type: none"> Service Planning 	
	Establishing appropriate key performance indicators (KPIs) as part of the planning process in order to identify how the performance of services and projects is to be measured.	<ul style="list-style-type: none"> Service Planning Performance Indicators Annual Report 	
	Ensuring capacity exists to generate the information required to review service quality regularly.	<ul style="list-style-type: none"> Performance indicators are reported, benchmarking is undertaken and corrective action taken where necessary 	
	Preparing budgets in accordance with organisational objectives, strategies and the medium term financial plan.	<ul style="list-style-type: none"> Budget Consultation Corporate Plan Medium Term Financial Plan Budget Report Executive Member Consultation 	
	Informing medium and long term resource planning by drawing up realistic estimates of revenue and capital expenditure aimed at developing	<ul style="list-style-type: none"> Corporate Plan Medium Term Financial Plan Budget Report 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	a sustainable funding strategy.		
Optimising achievement of intended outcomes	Ensuring the Medium Term Financial Plan integrates and balances service priorities, affordability and other resource constraints.	<ul style="list-style-type: none"> • Annual Budget Report • External Auditor Letter/Report 	
	Ensuring the budgeting process is all-inclusive, taking into account the full cost of operations over the medium and longer term.	<ul style="list-style-type: none"> • Budget Guidance • Officer/Executive Member Consultation 	
	Ensuring the Medium Term Financial Plan sets the context for ongoing decisions on significant delivery issues or responses to changes in the external environment that may arise during the budgetary period in order for outcomes to be achieved while optimising resource usage.	<ul style="list-style-type: none"> • Revenue/Capital Monitoring • Review of Medium Term Financial Plan 	
	Ensuring the achievement of 'social value' through service planning and commissioning. The Public Services (Social Value) Act 2012 states that this is "the additional benefit to the community...over and above the direct purchasing of goods, services and outcomes".	<ul style="list-style-type: none"> • Budget Report • Statement of Accounts 	

Principle E - Developing the entity's capacity, including the capability of its leadership and the individuals within it.

Local government needs appropriate structures and leadership, as well as people with the right skills, appropriate qualifications and mindset, to operate efficiently and effectively and achieve their intended outcomes within the specified periods. A local government organisation must ensure that it has both the capacity to fulfil its own mandate and to make certain that there are policies in place to guarantee that its management has the operational capacity for the organisation as a whole. Because both individuals and the environment in which an authority operates will change over time, there will be a continuous need to develop its capacity as well as the skills and experience of the leadership of individual staff members. Leadership in local government entities is strengthened by the participation of people with many different types of backgrounds, reflecting the structure and diversity of communities.

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
Developing the entity's capacity	Reviewing operations, performance use of assets on a regular basis to ensure their continuing effectiveness.	<ul style="list-style-type: none"> Revenue/Capital Monitoring Service Reviews Performance Reports 	
	Improving resource use through appropriate application of techniques such as benchmarking and other options in order to determine how the authority's resources are allocated so that outcomes are achieved effectively and efficiently.	<ul style="list-style-type: none"> Benchmarking undertaken where applicable. 	
	Recognising the benefits of partnerships and collaborative working where added value can be achieved.	<ul style="list-style-type: none"> Health and Social Care Partnership Board Healthier Together Joint Committee Strategic Commissioning Board Tameside Adults Safeguarding Partnership Board Tameside Children Safeguarding Board 	
	Developing and maintaining an effective workforce plan to enhance the	<ul style="list-style-type: none"> Workforce Plan Service Plans Organisational Development Plan (Getting into 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	strategic allocation of resources.	Gear)	
Developing the capability of the entity's leadership and other individuals	Developing protocols to ensure that elected and appointed leaders negotiate with each other regarding their respective roles early on in the relationship and that a shared understanding of roles and objectives is maintained.	<ul style="list-style-type: none"> • Job Descriptions • Member Portfolios • Constitution Article 16 - Officers • Constitution - Appointment of Statutory and Proper Officers 	
	Publishing a statement that specifies the types of decisions that are delegated and those reserved for the collective decision making of the governing body.	<ul style="list-style-type: none"> • Constitution – Article 17 Decision Making • Constitution - Terms of Reference and Scheme of Delegation • Financial Regulations • Procurement Standing Orders 	
	Ensuring the leader and the chief executive have clearly defined and distinctive leadership roles within a structure whereby the chief executive leads the authority in implementing strategy and managing the delivery of services and other outputs set by members and each provides a check and a balance for each other's authority.	<ul style="list-style-type: none"> • Member Portfolios • Constitution Article 16 - Officers • Constitution - Appointment of Statutory and Proper Officers 	
	Developing the capabilities of members and senior management to achieve effective shared leadership and to enable the organisation to respond successfully to changing legal and policy demands as well as economic,	<ul style="list-style-type: none"> • Annual Development Reviews • Member Development • Organisational Development (Getting into Gear • Induction programme for Staff • Induction programme for Members 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	<p>political and environmental changes and risks by:</p> <ul style="list-style-type: none"> ensuring members and staff have access to appropriate induction tailored to their role and that ongoing training and development matching individual and organisational requirements is available and encouraged. ensuring members and officers have the appropriate skills, knowledge, resources and support to fulfil their roles and responsibilities and ensuring that they are able to update their knowledge on a continuing basis. ensuring personal, organisational and system wide development through shared learning, including lessons learnt from governance weaknesses both internal and external. 	<ul style="list-style-type: none"> Member/Senior Officer Development Days Scrutiny Panels 	
	Ensuring that there are structures in place to encourage public participation.	<ul style="list-style-type: none"> Town Councils The Big Conversation Citizen Magazine Partnership Engagement Network 	
	Taking steps to consider the leadership's own effectiveness and ensuring leaders are open to constructive feedback from peer review	<ul style="list-style-type: none"> Annual Development Reviews Supervision Meetings Executive Member Annual Reports 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	and inspections.		
	Holding staff to account through regular performance reviews which take account of training or development needs.	<ul style="list-style-type: none"> • Annual Development Reviews • Supervision Meetings • Organisational Development – Getting into Gear 	
	Ensuring arrangements are in place to maintain the health and wellbeing of the workforce and support individuals in maintaining their own physical and mental wellbeing.	<ul style="list-style-type: none"> • Health and Wellbeing pages on Staff Portal • Chief Executive's Brief • The Wire • Strive Management Development Programme 	

Principle F - Managing risks and performance through robust internal control and strong public financial management.

Local government needs to ensure that the organisations and governance structures that it oversees have implemented, and can sustain, an effective performance management system that facilitates effective and efficient delivery of planned services. Risk management and internal control are important and integral parts of a performance management system and crucial to the achievement of outcomes. Risk should be considered and addressed as part of all decision making activities. A strong system of financial management is essential for the implementation of policies and the achievement of intended outcomes, as it will enforce financial discipline, strategic allocation of resources, efficient service delivery, and accountability. It is also essential that a culture and structure for scrutiny is in place as a key part of accountable decision making, policy making and review. A positive working culture that accepts, promotes and encourages constructive challenge is critical to successful scrutiny and successful delivery. Importantly, this culture does not happen automatically, it requires repeated public commitment from those in authority.

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional work Identified
Managing risk	Recognising that risk management is an integral part of all activities and must be considered in all aspects of decision making.	<ul style="list-style-type: none"> • Risk Management Policy and Strategy • All reports to Council, Panels and Committees have to include risk management comments. 	
	Implementing robust and integrated risk management arrangements and ensuring that they are working effectively.	<ul style="list-style-type: none"> • Risk Management Policy and Strategy reviewed annually. 	
	Ensuring that responsibilities for managing individual risks are clearly allocated	<ul style="list-style-type: none"> • Risk Management Policy and Strategy 	
Managing performance	Monitoring service delivery effectively including planning, specification, execution and independent post implementation review.	<ul style="list-style-type: none"> • Service Plans • Performance indicators • Budget Monitoring • Benchmarking 	
	Making decisions based on relevant,	<ul style="list-style-type: none"> • Publication of agendas and minutes of 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional work Identified
Page 71	clear objective analysis and advice pointing out the implications and risks inherent in the organisation's financial, social and environmental position and outlook	<p>meetings</p> <ul style="list-style-type: none"> • All reports to Council, Panels and Committees have to include legal, financial and risk management comments. • Agenda Preparation Timetables in place. 	
	Ensuring an effective scrutiny or oversight function is in place which encourages constructive challenge and debate on policies and objectives before, during and after decisions are made thereby enhancing the organisation's performance and that of any organisation for which it is responsible (OR, for a committee system) Encouraging effective and constructive challenge and debate on policies and objectives to support balanced and effective decision making.	<ul style="list-style-type: none"> • Scrutiny Function • Agendas and minutes of Scrutiny Panels • Scrutiny Panel Terms of Reference • Forward Plan • Scrutiny Annual Report • Constitution – Article 17 Decision Making 	
	Providing members and senior management with regular reports on service delivery plans and on progress towards outcome achievement.	<ul style="list-style-type: none"> • Agenda Preparation Timetable • Constitution - Access To Information Procedure Rules 	
	Ensuring there is consistency between specification stages (such as budgets) and post implementation reporting (e.g. financial statements).	<ul style="list-style-type: none"> • Financial Regulations • Procurement Standing Orders • Revenue/Capital Monitoring • Strategic Planning and Capital Monitoring Panel 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional work Identified
Robust internal control	Aligning the risk management strategy and policies on internal control with achieving the objectives.	<ul style="list-style-type: none"> • Risk Management Policy and Strategy • Audit Plan • Audit Reports 	
	Evaluating and monitoring the authority's risk management and internal control on a regular basis.	<ul style="list-style-type: none"> • Audit Plan • Risk Management Policy and Strategy reviewed annually • Progress Reports presented to the Audit Panel • Annual Report from Head of Risk Management and Audit Services 	
	Ensuring effective counter fraud and anti-corruption arrangements are in place.	<ul style="list-style-type: none"> • Fraud function compliant with the Code of Practice on Managing the Risk of Fraud and Corruption (CIPFA 2014) 	
	Ensuring additional assurance on the overall adequacy and effectiveness of the framework of governance, risk management and control is provided by the internal auditor.	<ul style="list-style-type: none"> • Annual Governance Statement • Public Sector Internal Audit Standards • Progress Reports presented to the Audit Panel • Annual Report from Head of Risk Management and Audit Services 	
	Ensuring an audit committee or equivalent group or function which is independent of the executive and accountable to the governing body: <ul style="list-style-type: none"> • provides a further source of effective assurance regarding arrangements for managing risk and maintaining an effective control environment • that its recommendations are listened to and acted upon. 	<ul style="list-style-type: none"> • Audit Panel Terms of Reference • Agendas and Minutes published 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional work Identified
Managing data	Ensuring effective arrangements are in place for the safe collection, storage, use and sharing of data, including processes to safeguard personal data.	<ul style="list-style-type: none"> Information Governance Framework Information Governance Group 	
	Ensuring effective arrangements are in place and operating effectively when sharing data with other bodies.	<ul style="list-style-type: none"> Data Sharing Protocol Advice from Legal and Risk Management provided Project Groups established 	
	Reviewing and auditing regularly the quality and accuracy of data used in decision making and performance monitoring.	<ul style="list-style-type: none"> Internal Audit Plan 	
Strong public financial management	Ensuring financial management supports both long term achievement of outcomes and short-term financial and operational performance.	<ul style="list-style-type: none"> Medium Term Financial Plan Budget report Revenue/Capital Monitoring All reports presented to Council, Panels and Committees require Financial Comments 	
	Ensuring well-developed financial management is integrated at all levels of planning and control, including management of financial risks and controls.	<ul style="list-style-type: none"> Qualified Managers in post. Budget report Financial Business Partners work with Directorates Revenue/Capital Monitoring Internal Audit Reports External Audit Letter/Report 	

Principle G - Implementing good practices in transparency, reporting, and audit to deliver effective accountability.

Accountability is about ensuring that those making decisions and delivering services are answerable for them. Effective accountability is concerned not only with reporting on actions completed, but also ensuring that stakeholders are able to understand and respond as the organisation plans and carries out its activities in a transparent manner. Both external and internal audit contribute to effective accountability.

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
Implementing good practice in transparency	Writing and communicating reports for the public and other stakeholders in an understandable style appropriate to the intended audience and ensuring that they are easy to access and interrogate.	<ul style="list-style-type: none"> • Council Website • Transparency Pages • Annual reports 	
	Striking a balance between providing the right amount of information to satisfy transparency demands and enhance public scrutiny while not being too onerous to provide and for users to understand.	<ul style="list-style-type: none"> • Statement of Accounts • Annual Report 	
Implementing good practices in reporting	Reporting at least annually on performance, value for money and the stewardship of its resources.	<ul style="list-style-type: none"> • External Audit Letter/Report • Statement of Accounts • Annual Report 	
	Ensuring members and senior management own the results.	<ul style="list-style-type: none"> • Minutes of Meetings • Job Descriptions • Member Portfolios 	
	Ensuring robust arrangements for assessing the extent to which the principles contained in the Framework have been applied and publishing the	<ul style="list-style-type: none"> • Annual Governance Statement 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	results on this assessment including an evidence to demonstrate good governance (annual governance statement).		
	Ensuring that the Framework is applied to jointly managed or shared service organisations as appropriate.	<ul style="list-style-type: none"> Annual Governance Statement 	
	Ensuring the performance information that accompanies the financial statements is prepared on a consistent and timely basis and the statements allow for comparison with other similar organisations.	<ul style="list-style-type: none"> Statement of Accounts External Audit Letter/Report Deadlines in place Qualified officers in post 	
Assurance and effective accountability	Ensuring that recommendations for corrective action made by external audit are acted upon.	<ul style="list-style-type: none"> Minutes from Executive Cabinet/Audit Panel Meeting Internal Audit Plan 	
	Ensuring an effective internal audit service with direct access to members is in place which provides assurance with regard to governance arrangements and recommendations are acted upon.	<ul style="list-style-type: none"> Internal Audit - Post Audit Reviews Progress Reports presented to the Audit Panel Annual Report from Head of Risk Management and Audit presented to Audit Panel 	
	Welcoming peer challenge, reviews and inspections from regulatory bodies and implementing recommendations.	<ul style="list-style-type: none"> Action plans are formulated to ensure recommendations are implemented, e.g. Ofsted Inspection of Childrens Services. 	
	Gaining assurance on risks associated with delivering services through third	<ul style="list-style-type: none"> Annual Governance Statement 	

Supporting Principles	Behaviours and Actions that Demonstrate Good Governance in Practice	Evidence to Support Compliance	Additional Work Identified
	parties and that this is evidenced in the annual governance statement.		
	Ensuring that when working in partnership, arrangements for accountability are clear and that the need for wider public accountability has been recognised and met.	<ul style="list-style-type: none"> • Specific Partnership Agreements • Partnership Boards 	

DRAFT

Annual Governance Statement
2017/2018

This is a signed statement by the Executive Leader and Chief Executive certifying that governance arrangements are adequate and operating effectively within the Council.

1. Scope of Responsibility

Tameside MBC (the Council) is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively. The Council also has a duty under the Local Government Act 1999 to make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness.

In discharging this overall responsibility, the Council is also responsible for putting in place proper arrangements for the governance of its affairs, facilitating the effective exercise of its functions, which includes arrangements for the management of risk. These arrangements are intended to make sure that we do the right things, in the right way, for the right people, in good time, and in a fair, open, honest and accountable way. The Council has approved and introduced a Code of Corporate Governance.

This Annual Governance Statement explains how we have followed the above Code and the requirements of the Accounts and Audit (England) Regulations 2015.

The Council, in accordance with the Local Government Pension Scheme (LGPS) Regulations, which are written by the Department for Communities and Local Government (DCLG) and passed by Parliament, administers the Greater Manchester Pension Fund (GMPF).

The Council delegates the function in relation to maintaining the GMPF to the following:-

- Pension Fund Management Panel
- Pension Fund Advisory Panel
- Pension Fund Working Groups
- The Executive Director of Pensions
- The Local Board

The Executive Leader of the Council chairs the Management Panel and all Panels and Working Groups have elected members from the other nine Greater Manchester Authorities, as the fund is accountable to its member Authorities. The Local Board has an equal number of scheme employer and scheme member representatives. Whilst the GMPF has different governance arrangements to other Council Services (which are all detailed on its website), all officers are employees of the Council and therefore comply with the Council's Code of Corporate Governance and Constitution. Specific reference will not be made to GMPF throughout the Annual Governance Statement, unless appropriate to do so, as it is considered to be part of the Council.

2. The Purpose of the Governance Framework

The Governance Framework comprises the systems and processes, and culture and values by which the Council is directed and controlled and its activities through which it accounts to, engages with and leads the community. It enables the Council to monitor the achievement of its strategic objectives and to consider whether those objectives have led to the delivery of appropriate, cost effective, services.

The system of internal control is a significant part of the framework and is designed to manage risk to a reasonable level. It cannot eliminate all risk of failure to achieve policies, aims and objectives and can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify and prioritise the risks to the achievement of the Council's policies, aims and objectives, to evaluate the likelihood of

those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically.

The Governance Framework has been in place at the Council for the year ending 31 March 2018, and up to the date when the annual accounts are approved.

3. The Governance Framework

Developing codes of conduct which define standards of behaviours for members and staff and policies dealing with whistleblowing and conflicts of interest and that these codes and policies are communicated effectively.

Members and Officers are governed by Codes of Conduct, Cabinet Portfolios, contracts of employment, employment rules and procedures, Professional Codes of Conduct and bound by the Constitution and Code of Corporate Governance. Conflicts of interest are recorded in the minutes of all meetings, where applicable, and a register is maintained for both members and officers by the Monitoring Officer.

The Council is committed to leading on and maintaining the highest standards of behaviour and in support of this hosts and chairs the National Anti-Fraud Network (NAFN). In addition to those mentioned above, documentation to eliminate corruption includes Procurement Standing Orders, Financial Regulations, Anti-Fraud, Bribery and Corruption: Statement of Intent, Terms of Reference, Protocols for Gifts and Hospitality and Standards of Conduct and Ethics.

The Council has a published Whistleblowing Policy on its public website and awareness and updates are provided in its internal communications magazine, the Wire. Allegations received are investigated by either the Monitoring Officer or Internal Audit.

Such guidance is accompanied by training and communications. The work of the Monitoring Officer, Standards Committee and the Standards Panel are fundamental in defining, achieving and monitoring high standards.

Ensuring compliance with relevant law and regulations, internal policies and procedures, and that expenditure is lawful.

All reports to Senior Managers, Board, Panels, Working Groups, Council and for Key/Executive Decisions are subject to review by the Executive Director of Governance and Pension, as the Monitoring Officer and the Director of Finance, as the Section 151 Officer. Internal Audit assesses compliance with internal policies and procedures on an ongoing basis and annually all members of the Single Leadership Team sign an Assurance Statement and complete a self-assessment checklist, which includes questions on the above issues.

Standing Orders, Financial Regulations and the Scheme of Delegation are all reviewed and updated regularly and presented to the Council for approval. All decisions of the Council are minuted and available on the website. Supporting procedure notes/manuals to manage risks and ensure consistency of approach are updated regularly and checked as part of the internal audit process. All managers receive regular legal updates from the Director of Governance and Pensions via a Lawyers in Local Government Bulletin.

The Medium Term Financial Plan, the Budget Report and a detailed monitoring regime for both revenue and capital expenditure, together with the Section 151 Officer and Monitoring Officer, ensures that expenditure is lawful. Officers of the Council are well trained, competent in their areas of expertise and governed by rules and procedures. Officers have regular supervision meetings to ensure that performance is satisfactory and the attendance at training seminars/courses ensures that officers are up to date with developments in their areas of expertise.

Documenting a commitment to openness and acting in the public interest.

The Council's Constitution - Access to Information Procedure Rules outlines access to Council meetings, agendas and minutes, so that members of the public can be involved in the governance arrangements of the Council.

In response to the government's desire for increased transparency, the Local Government Transparency Code was published in October 2014 and the Council now produces open data, examples of which are; Expenditure over £500, procurement information, payment of undisputed invoices within 30 days, members allowances, salaries and wages information and fraud data. The Council also respond to Freedom of Information requests and has a central monitoring system in place to ensure deadlines are achieved.

Tameside also has a number of Town Councils in place which allow members of the public to participate in the decision making process and the Big Conversation which provides residents and service users the opportunity to express their views and opinions about the services they use and how they can be delivered.

Developing and communicating a vision which specifies intended outcomes for citizens and service users and is used as a basis for planning.

The Council needs to set out a clear vision that members, employees and the public can identify with and help deliver as public services are changing rapidly due to new legislation and funding cuts. The vision detailed below is set out in the Corporate Plan 2016/21 which can be found [here](#).

The Council as a representative body exists to maximise the wellbeing and health of the people within the borough:-

- Supporting economic growth and opportunity;
- Increasing self-sufficiency and resilience of individuals and families; and
- Protecting the most vulnerable.

Everything the Council does will aim to make this vision a reality by focusing resources on what matters. The core purpose and values put people at the forefront of services to ensure that every decision made supports economic growth and self-sufficiency. The aim is to work with residents by asking them to take on greater responsibility in their families, communities and area, supporting them when they need help.

The Council is currently revising its Corporate Plan and will publish a refreshed corporate plan in June 2018.

No one organisation can achieve the change aimed for on its own. The Council and its partners are committed to working together along with the people of Tameside to achieve lasting change for the borough.

The Care Together Programme Board was established in summer 2015, to ensure the smooth transition from the current to the new system of health and care. Its responsibilities include managing risks; ensuring patient quality and safety is at the heart of all the changes, overseeing the development of the models of care and engaging staff and the public. The Board meets on a regular basis and reports to the Health and Wellbeing Board, the body responsible for improving the health and wellbeing of the people of Tameside and Glossop.

The landscape the Council operates in has changed significantly over the last 5 years and this has impacted significant on how the Council delivers against its objectives. In 2016 the Government offered any council that wished to take it up, a four year funding settlement to 2019/20, making a commitment to provide minimum funding allocations for each year of the Spending Review period. This offer was subject to the Council choosing to accept the offer and publishing an efficiency plan

by October 2016, which the Council accepted. The four year funding settlement provides the Council with greater certainty over its funding allocations to the end of 2019/20 which enables service planning to take place with more certainty. However, the position beyond 2020 falls outside of this four year settlement and no indicative information is yet available for future periods. This coupled with the Government's commitment to review the way that local government is funded through its Fair Funding review, creates further uncertainty that the Council needs to be aware of, and factor into its financial assumptions.

The Localism Act and the Care Act have all had implications for the work of the Council.

The development of the Council's strategic approach through the Corporate Plan has been informed by a number of factors not least the following (although this list is not exhaustive):-

- Ongoing engagement between the Council and local people;
- Budget Consultation ;
- Big Conversation – service specific consultations to inform service redesign;
- Public Service Reform;
- Greater Manchester Devolution Agreement;
- Greater Manchester Health and Social Care Devolution;
- Care Together (health and social care integration);
- Medium Term Financial Plan;
- Vision Tameside; and
- Greater Manchester Strategy.

Translating the vision into courses of action for the Council, its partnerships and collaborations.

The Tameside Corporate Plan 2016/21 is the Borough's plan to maximise the wellbeing and health of the people within the Borough. Working with partners across public services, industry, commerce, the community and voluntary sectors the vision is translated into objectives which are detailed service plans, team plans, and individual development plans.

The Council is currently revising its Corporate Plan and will publish a refreshed corporate plan in June 2018.

The Care Together Programme and the creation of an integrated system of health and social care brings together Tameside and Glossop Clinical Commissioning Group, Tameside Metropolitan Borough Council and Tameside and Glossop Integrated Care NHS Foundation Trust to reform health and social care services to improve the health outcomes of our residents and reduce health inequalities.

Vision Tameside and Ashton Old Baths are examples of the major projects that the Council has, and is continuing to deliver, with partners that demonstrate that it has translated its vision into objectives. The Council is working with Price Waterhouse Coopers (PWC) the administrator for Carillion to ensure that the Vision Tameside project is completed following the collapse of Carillion.

Educational attainment levels in Tameside are a key priority and 62% of KS4 pupils achieved the standard in English and Maths, progress is in line with the previous year, but a rise in numbers achieving the EBACC. At KS2 there was a rise of 5% to 60% achieving the expected standard in reading, writing and maths – and progress above the national average was achieved in writing and maths.

The GMPF helps to support the Council's vision and its objectives are detailed in service plans which are presented to Working Groups and the Management/Advisory Panel. In conjunction with West Yorkshire Pension Fund and Merseyside Pension Fund the Northern Pool has been approved by Government and will become operational from April 2018. It creates a £35+ billion asset pool, providing greater scope to allow the funds to invest in major regional and national infrastructure projects.

Establishing clear channels of communication with all sections of the community and other stakeholders, ensuring accountability and encouraging open consultation.

Significant improvements in the quality of life for our residents will only be achieved through effective partnership working. This involves working together through a shared vision for the future of the borough, to create a prosperous economy where people learn and achieve, feel safe and healthy, and, take active responsibility for their environment.

The Corporate Plan is the key document that communicates the vision for Tameside, and the delivery of the vision is supported by outcome specific networks, joint teams and partnerships.

The Council is currently revising its Corporate Plan and will publish a refreshed corporate plan in June 2018.

In addition to the website, the Council has embraced social media (Facebook, Twitter and Instagram) as modern communication channels to endeavour to reach all sections of the community. Council meetings are webcast and the Executive Leader and Executive Members publish Blogs on the Council's website.

The Tameside Engagement Strategy sets out the way the Council will involve local people in shaping delivery of high quality services across the borough. It aims to help ensure that a co-ordinated and strategic approach to consultation and engagement is undertaken.

Consultation has continued using the Big Conversation which provides residents and service users the opportunity to express their views and opinions about the services they use and how they can be delivered in the future, in light of the financial challenges faced by Tameside.

The Council has refreshed its approach to consultation and engagement and now has in place a comprehensive Partnership Engagement Network which brings together stakeholders from a range of organisations and groups to inform and influence policy development and decision making.

Accountability is demonstrated by the publication of the Statement of Accounts, the Annual Report in the Citizen Newspaper, the Annual Governance Statement and the review of service plans and the People and Places Scorecard.

Reviewing the effectiveness of the decision-making framework, including delegation arrangements, decision-making in partnerships, information provided to decision makers and robustness of data quality.

The Council has a well-defined decision-making process and Scheme of Delegation, which are documented in the Constitution. It publishes a Forward Plan and all agendas and minutes of meetings can be found on the Council's public website. The Safe and Sound Decision Making Framework in place ensures that good processes are in place for making and implementing decisions, which are informed by good information and data, stakeholder views and an open and honest debate, which reflects the interests of the community.

The robustness of data quality is the responsibility of managers and is reviewed as part of the Internal Audit and External Audit functions. Performance indicators, which are collated centrally, are regularly reported to the Single Leadership Team. Intelligence reviews focused on addressing specific issues of focus or concern are regularly produced and have in the last twelve months included Look after Children and the impact of welfare reform. Performance reports are provided to the strategic commissioning board on a bi-monthly

Measuring the performance of services and related projects and ensuring that they are delivered in accordance with defined outcomes and that they represent the best use of resources and value for money.

Effective challenge is an integral part of how the Council and its partners manage Tameside. It ensures that the partnership and constituent organisations remain focused on improvement and achievement. Challenge helps to identify areas for benchmarking and the development of best practice. Similarly, it supports individuals and teams further develop their own skills and capacity, which in turn helps to deliver better outcomes for local people.

The Council's approach includes:-

- Peer assessment and challenge;
- Performance Management;
- Big Conversation and Service Redesign;
- Scrutiny, and
- Risk Management.

Continual improvement has always been at the heart of the organisation and the results can be seen through our sustained record of achievement. In the External Auditor's Audit Letter dated October 2017, the Council received a qualified Value for Money conclusion due to the Inadequate Ofsted judgement on Children's Services which was published in December 2016. ,

The letter also stated that:-

- "The Council is responding well to the findings of Ofsted in December 2016 which rated Children's Services as Inadequate. An Improvement Plan has been developed with the creation of an independently chaired multi-agency Children's Services Improvement Board to oversee progress.
- The Council has maintained a tight control of its budget and net expenditure at 31 March 2017 was £8.376m less than plan. The medium term financial plan, approved by the Council in February 2017, extends to 2019/20 and requires a further £14.4m of cost savings to be achieved. This is a challenge to the Council given the increase in demand for services and future funding reductions.
- The Council has also continued to invest in the Borough with £35.288m capital spend during the year.
- The Council is making good progress with the delivery of the Care Together programme, together with the local CCG and NHS Foundation Trust, to transform healthcare in Tameside and Glossop. Resources were pooled into a single Integrated Commissioning Fund (ICF) underpinned by a financial framework which became fully operational on 1 April 2016. The ICF enables single commissioning arrangements for healthcare with decisions made at a Single Commissioning Board."

The Value for Money conclusion assessed by External Audit is based on one single criterion for auditors to evaluate:-

- In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

While planning for the future we remain focused on the present. The need to balance the budget focuses us on service redesign. We ensure service users are engaged and involved, and services they rely on are safeguarded wherever possible. Our Customer Service Excellence award is testament. Tameside gained 100% compliance against all criteria, and eight areas of compliance plus – a discretionary award for 'exceptional best practice'. The report stated "... continued to improve and focus on the development and delivery of customer-focussed services, despite the continuing financial challenges..."

GMPF is leading the way in investment and pooling innovation, particularly in the areas of housing and infrastructure development. Airport City is a joint venture between GMPF, Manchester Airport Group, Carillion and Beijing Construction Engineering Group. The partners are developing over 5

million square feet of hotels, offices, manufacturing, logistics and retail space directly adjacent to Manchester Airport, an ideal gateway to carry out business throughout the UK, Europe and the world.

Defining and documenting the roles and responsibilities of members and management with clear protocols for effective communication in respect of the Council and partnership arrangements.

The Council Constitution sets out the roles and responsibilities of each Executive Member, and the responsibilities delegated to the Chief Executive, members of the Single Leadership Team and senior managers of the Council. It includes the post and responsibilities of the Statutory and Proper Officers.

The Chief Executive for the Council is the Accountable Officer for the Tameside and Glossop Clinical Commissioning Group and joint management arrangements have continued to develop during 2017/18 to foster closer working. Some service areas like People and Workforce Development and Policy, Performance and Communications are delivering services directly to the Tameside and Glossop Clinical Commissioning Group.

Protocols for effective communication are in place. Meetings have agendas and minutes published on the Council's Website and a Forward Plan is published. The Executive Leader's Annual Key Note Address, the Corporate Plan, the Citizen Magazine, Scrutiny, Consultation via the Big Conversation and, increasingly, the use of Social Media (Facebook, Twitter and Instagram) are examples of how the Council communicates with partners and residents of the Borough.

The constitution is reviewed and updated regularly and changes are disseminated across the Council and Tameside and Glossop Clinical Commissioning Group via the Steven's Weekly Brief, The Wire and team briefings.

The Tameside Health and Wellbeing Board is a statutory partnership with health commissioners, providers and other interested parties. It is chaired by the Executive Leader of the Council and has developed the Tameside Health and Wellbeing Strategy that identifies priorities to address local health inequalities.

Ensuring that financial management arrangements conform with the governance requirements of the CIPFA Statement on the Role of the Chief Finance Officer in Local Government (2015) and where they do not, explain why and how they deliver the same impact.

The financial management arrangements in place conform with the CIPFA statement and the service was managed by the Assistant Executive Director of Finance until 30 September 2017, thereafter from 1 October 2017 a Director of Finance was appointed which is shared with the Tameside and Glossop Clinical Commissioning Group, acting as the Council's Section 151 Officer, up to 31 March 2018. The role is supported by Assistant Director of Finance on the Council side and a Deputy Chief Finance Officer supporting the Clinical Commissioning Group.

Ensuring effective arrangements are in place for the discharge of the monitoring officer function.

The Executive Director of Governance and Pensions) is the Monitoring Officer for the Council and the function is detailed in the Constitution. A Monitoring Officer Protocol is in place and detailed on the website.

Ensuring effective arrangements are in place for the discharge of the head of paid service function.

The Chief Executive is the head of paid service and the role and function are detailed in the Constitution.

Providing induction and identifying the development needs of members and senior officers in relation to their strategic roles, supported by appropriate training.

Induction guidelines are available for managers including a checklist to ensure consistency across all services. Member induction is delivered by the Monitoring Officer and the Executive Support Team.

Training needs are assessed using Annual Development Reviews for officers. The process takes into account the needs of the service and then identifies any gaps in the skills and knowledge of the workforce to enable it to meet its objectives. All training requirements are reviewed by management and then compiled into service training plans, which are submitted to People and Workforce Development to inform and direct the provision of future training and development opportunities.

Training for members is assessed on an annual basis and a programme of events is scheduled to ensure both local and national subjects are covered.

Reviewing the effectiveness of the framework for identifying and managing risks and for performance and demonstrating clear accountability.

The Council empowers its employees to be innovative and to find solutions to problems, but recognises that there are potential risks for the Council. As part of the Service Planning process, individual services develop their own risk registers and monitor controls. Significant and cross cutting service risks are amalgamated into the Corporate Risk Register. Every report presented to Senior Managers, Council, Committees, Board, Panels, Working Groups and for Key/Executive Decisions is risk assessed. The risk management process embraces best practice.

The Information Governance Framework which was introduced in November 2013 and refreshed during 2016 continued to be a key priority for the Council ensuring that the guidance contained in the supporting documents was relevant, disseminated and embedded across all service areas in light of the introduction of the General Data Protection Regulations (GDPR) and the new Data Protection Act in May 2018. The Information Governance Group, which was chaired by the Director of Governance and Pensions), ensured that available resources were directed towards compliance with the new legislation and in line with the requirements of the Information Commissioners Office, the regulatory body for enforcing the requirements of Data Protection legislation. Information Governance, Risk Management and Data Protection training is delivered via a range of media, including briefing notes, the Chief Executive's Briefing, the Wire, workshops, DVD's and E-Tutorials.

Ensuring effective counter fraud and anti-corruption arrangements are developed and maintained in accordance with the Code of Practice on Managing the Risks of Fraud and Corruption (CIPFA 2014).

The Council has an Anti-Fraud, Bribery and Corruption Strategy: Statement of Intent as part of the Constitution and all investigations are undertaken by Internal Audit. All investigations are conducted in line with the Fraud Response Plan and operational guidance notes. The Standards Panel receives regular reports on investigations underway to monitor progress and provide direction, where appropriate. The Council continues to participate in the National Fraud Initiative, which is coordinated by Internal Audit.

A Whistleblowing Policy is maintained and available on the Council's website.

Ensuring an effective scrutiny function is in place.

This role is performed both by the Scrutiny function and by Tameside Members who sit on Outside Bodies' Committees. The Scrutiny function conducts reviews across Tameside which may call into account other public service providers like the NHS. Reviews conducted are reported to the Scrutiny Panels and the Overview (Audit) Panel and the programme of reviews and reports are available on the scrutiny website together with an Annual Report. Members who represent the Council on outside bodies are ensuring that service delivery is effective, providing a challenge function and that the needs of Tameside are taken into account.

Ensuring that assurance arrangements conform with the governance requirements of the CIPFA Statement on the Role of the Head of Internal Audit (2010) and, where they do not, explain why and how they deliver the same impact.

The Council's assurance arrangements conform with the governance requirements of the CIPFA Statement. The Head of Risk Management and Audit Services reported directly to the Assistant Director of Finance until September 2017 and the Director of Finance from October 2017 as the Section 151 Officer. They also presented on a quarterly basis to the Audit Panel and the Greater Manchester Pension Fund Local Board. The Risk Management and Audit Services was also judged to conform to the Public Sector Internal Audit Standards following an External Peer Review conducted by Blackpool and Bolton Councils in accordance with the Memorandum of Understanding approved by all members of the North West Chief Audit Executive Group.

Undertaking the core functions of an Audit Committee, as identified in Audit Committees: Practical Guidance for Local Authorities and Police (CIPFA 2013).

The Audit Panel does comply with the guidance issued by CIPFA and is regularly attended by our External Auditor. Training is assessed for members of the panel based on their existing skills and knowledge.

Ensuring that the Council provides timely support, information and responses to external auditors and properly considers audit findings and recommendations.

Information, support and responses are provided to External Audit in a timely manner. Audit findings and recommendations are considered by the Director and Assistant Director of Finance, the Director of Governance and Pensions and the Assistant Director (Pensions Local Investments and Property) and presented to the Audit Panel, Overview (Audit) Panel, Executive Cabinet and the Pension Fund Management Advisory Panel.

In their Annual Letter of October 2017, Grant Thornton commented that:

"The Council made the first draft version of the accounts available for audit in line with the agreed timetable, although subsequent iterations were required. The Finance Team responded promptly and efficiently to our queries during the audit."

Incorporating good governance arrangements in respect of partnerships and other joint working and ensuring that they are reflected across the Council's overall governance structures.

Good governance arrangements in respect of partnership working were established many years ago when the Tameside Strategic Partnership was created and those standards are still adopted today.

The continued successful delivery of outcomes by the various networks, joint teams and partnerships operating across Tameside to maximise the wellbeing and health of the people of the Borough demonstrates that the arrangements in place are sound. Tameside has always promoted working with partners and it is through our strong and long-standing partnerships, along with new ones that may develop in the future, that help us to produce solutions and real improvements for

Tameside. Joint working with the Tameside and Glossop Clinical Commissioning Group, the joint appointments of the Chief Executive as the Accountable Officers and a shared Director of Finance, a shared Single Leadership Team are testament to this approach. Joint meetings/arrangements are also in place with Integrated Care Foundation Hospital Trust to ensure the Care Together Programme realises the benefits to the people of Tameside and Glossop.

4. Review of Effectiveness

The Council has responsibility for conducting, at least annually, a review of the effectiveness of its Governance Framework including the system of internal control. This review of effectiveness is informed by the work of the Directors/Assistant Directors within the Council who have responsibility for the development and maintenance of the governance environment, the Head of Risk Management and Audit Service's Annual Report, and by comments made by the External Auditor and other review agencies and inspectorates.

The process that has been applied in maintaining and reviewing the effectiveness of the Governance Framework includes the following measures and actions:-

- The Council has adopted a Planning and Performance Framework and carries out a programme of monitoring which runs throughout its annual cycle. This includes quarterly monitoring of all budgets and regular monitoring of Service Delivery Plans.
- The Corporate Plan is refreshed regularly to take into account changes in circumstances and need. These reviews are influenced from the outcomes of the Business Days held between the Executive Cabinet and the Single Leadership Team. The full refresh is currently underway with a revised Corporate Plan to be published in June 2018.
- The Capital Programme is regularly monitored and reported to the Strategic Planning and Capital Monitoring Panel, Overview (Audit) Panel and the Executive Cabinet.
- The Executive Cabinet carries out its functions in accordance with responsibilities outlined in Cabinet Portfolios, which are detailed in the Council's Constitution. Several Non-Executive Members are appointed to specific roles to assist Executive Members in the delivery of their particular areas of responsibility. All roles are assigned at the annual meeting of the Council.
- There is a well established Overview and Scrutiny function, which has been revised and updated in the light of experience. Scrutiny Panels review the work of the Council throughout the year; make a series of recommendations to Executive Cabinet, which then require a formal response and action, as appropriate. There is a public website where the public can access completed review reports and Annual Plans and Annual Reports.
- To support delivery of the Medium Term Financial Plan and be in a positive position to respond to the financial challenges facing the Council, a structured programme of service reviews/redesigns has continued during the year. The continuation of this work is necessary to ensure that we are in a strong position to manage and use our resources effectively to maintain good outcomes and achieve the level of savings required. Service areas are looking for new and innovative ways of doing things as well as working more closely with our partners. Given the magnitude of the tasks the Council faces, consultation via the Big Conversation has continued so that residents' views on any changes can be taken into consideration. The Director and Assistant Director of Finance have worked with the Executive Members/Single Leadership Team during the budget preparation period to ensure that a robust set of savings plans are in place and a clear delivery plan has been drawn up.

- The Directors have each reviewed the operation of key controls throughout the Council, from the perspective of their own directorates, using a detailed assurance self- assessment checklist. They have provided a signed assurance letter and identified any areas for improvement, which will form the basis of an action plan to this Governance Statement.
- The Code of Corporate Governance has been reviewed and the evidence documented to demonstrate compliance with the principles of good governance. The Review was reported to senior management and the Audit Panel in May 2018.
- The Director of Governance and Pensions as the Monitoring Officer, carried out a continuous review of all legal and ethical matters, receiving copies of all agendas, minutes, reports and associated papers, and commented on all reports that go to members and when necessary taking appropriate action, should it be required.
- The Director and Assistant Director of Finance as the Section 151 Officer, carried out a continuous review of all financial matters, receiving copies of all agendas, minutes, reports and associated papers, and commented on all reports that go to members and when necessary taking appropriate action, should it be required.
- The Standards Committee is responsible for standards and probity, and receives regular reports from the Director of Governance and Pensions, the Monitoring Officer.
- The role held by the Assistant Director of Finance from 1 April 2017 to 30 September 2017 and the Director of Finance from 1 October 2017 to 31 March 2018 conformed to the requirements of the five principles of the CIPFA Statement on the Role of the Chief Financial Officer (CFO) in Local Government.
- The report published by Ofsted in December 2016 on the Inspection of Children's Services in Tameside, which judged the service to be inadequate, highlighted a number of issues in relation to service delivery, leadership, management and governance and a detailed Improvement Plan has been created. Delivery of the Improvement Plan is overseen by the multi-agency Tameside Children's Services Improvement Board. The Board has an independent chair and an advisor from the Department for Education sits on the Board.
- The Audit Panel carries out an overview of the activities of the Council's Risk Management, Internal Audit and External Audit functions. Members are provided with a summary of reports issued and their associated audit opinion. They approve the Annual Plans for each, and receive regular progress reports throughout the year. The Head of Risk Management and Audit Services presents an Annual Report and opinion, and the External Auditor submits an Annual Audit Letter along with other reports during the year. The Corporate Risk Register was presented to the Audit Panel in March 2018.
- The Internal Audit Service provides a continuous review in accordance with the Council's obligations under the Local Government Act 1972, and the Accounts and Audit Regulations 2015. It operates under the Public Sector Internal Audit Standards and an External Peer Review conducted in March 2018 confirmed that the service is fully compliant with all the standards, and the assessment was reported to the Audit Panel in May 2018.
- The Information Governance Group has continued to monitor the Information Governance Action Plan, Freedom of Information and Subject Access Requests throughout the year to ensure that robust processes are in place and the all services are compliant with data protection legislation.
- The Council's External Auditors review the activities of the Council and issue an annual opinion on the Annual Accounts and a Value for Money conclusion. Conclusions and significant issues arising are detailed in their report to those charged with governance.

- Progress on the development areas identified in Section 5, are regularly reported to the Audit Panel throughout the year by the Head of Risk Management and Audit Services.

5. Level of Assurance

The governance arrangements in place comply with the Principles outlined in the Council's Code of Corporate Governance and can be regarded as fit for purpose. A few areas for development have been identified in the Action Plan attached at **Appendix A**, and addressing these will further enhance the Governance Framework.

Improvements arising from Internal/External Audit Reports and Inspection Reports have already been built into Service Area Action Plans and are monitored as part of the Performance Management Framework.

6. Conclusion and Signatures

The Annual Governance Statement has been reviewed by Senior Management, presented to the Audit Panel and approved by the Overview (Audit) Panel. We have been advised on the implications of the review of the effectiveness of the Governance Framework in place, and the action plan compiled to address the further developments identified to ensure the continual improvement of the system in place.

We are satisfied that these steps will address the improvements that have been identified and their implementation will be monitored by the Audit Panel throughout the year and as part of our next Annual Review.

Signed:

Signed:

.....
Councillor Brenda Warrington
Executive Leader of Tameside MBC

.....
Steven Pleasant MBE
Chief Executive of Tameside MBC


Dated: 30 July 2018

Dated: 30 July 2018

Area of Review	Improvement Required	Progress to Date	Improvement Owner and Completion Date
Carillion/Vision Tameside (Carry Forward)	This is a multi-million pound project in partnership with Tameside College, and needs to be delivered in accordance with agreed milestones. It is essential that the risks to service delivery during the interim period are kept under review to minimise disruption to the people and businesses of Tameside so that, together, the mutual benefits of the project will be recognised and celebrated. It is also important to ensure that the benefits of the new building are realised in terms of different ways of working and reducing future running costs.	<p>Carillion the main contractor engaged by the LEP to construct the Vision Tameside build went into Liquidation on 15 January 2018.</p> <p>The LEP proposed an 8 week Early Works Order with Robertson Construction commencing 14 February following a Cabinet decision taken by the Council on 9 February. The Early Works Order allowed Robertson's to carry out due diligence, re-engage sub contractors and enter into contact with the council to complete the build. The Early Works Order was extended for a further 4 weeks for negotiations and contractual issues to be resolved.</p> <p>Subject to contractual issues being resolved, a new programme has been developed to show completion of the building prior to Christmas 2018. All partner organisations are fully aware of the new programme.</p> <p>Additional costs to complete the building cannot be covered by contingency and the council will be required to identify further capital monies to complete the building. This will be subject to formal governance by end of May 2018.</p> <p>Progress reports will be submitted to the Strategic Planning and Capital Panel. The Chief Executive, Leader and appropriate Executive Members are updated on a weekly basis.</p> <p>PWC the official liquidators have been informed of the council's intentions.</p>	Director of Growth March 2019
Children's Services (Carry Forward)	Improvements in response to the Ofsted Inspection published in December 2016, which have been detailed in the Tameside Children's Services Improvement Plan, need	New leadership in place – Director of Children's Services (DCS), Assistant Director and two Heads of Service. New Improvement Plan signed off 30/11/2017. Further Ofsted Monitoring Visits in January and April 2018 have judged	Director of Children's Summer 2019

Area of Review	Improvement Required	Progress to Date	Improvement Owner and Completion Date
	to be implemented and an Improvement Board is in place to monitor progress.	the Council to have taken appropriate action to address the slow pace of improvement, and that the new leadership has accurate understanding of current state of service and what improvements are still required; still improvements required in casework, but progress being made including improved children's outcomes, accurate quality assurance and improved management oversight.	
Pension Fund Pooling of Investments (Carry Forward)	Greater Manchester Pension Fund is working with other large metropolitan LGPS funds to create a £45+ billion asset pool. Pooling of assets will provide greater scope to allow the funds to invest in major regional and national infrastructure projects such as airport expansion, major new road and rail schemes, housing developments and energy production growth, all driving economic growth and prosperity. Strong governance arrangements will need to be in place, underpinned by robust and resilient systems and procedures, to ensure the desired outcomes are realised.	<p>The three funds have established an investment vehicle, which makes collective direct infrastructure investments and collective private equity investments.</p> <p>A procurement exercise has been undertaken to appoint a pool custodian, and a commercial and legal review of the successful bidders' contract is currently ongoing.</p> <p>A formal joint committee governance structure will be established in May 2018.</p> <p>Representatives of the Fund will continue to work closely and seek professional advice, as required, in order to finalise all aspects of the Pool.</p>	<p>Director of Governance and Pensions</p> <p>March 2019</p>
Health and Safety (Carry Forward)	To Review process and procedures in place to ensure consistency of approach and embrace electronic recording where appropriate.	<p>Directorate Health and Safety Meetings now established to ensure consistency of approach across the organisation.</p> <p>Health and Safety Service redesign taken to April Employer Consultation Group with agreement for a new Service Manager to be appointed. A full audit of all aspects of the Council to be commissioned and then a new service established with electronic accident reporting.</p> <p>Recruitment to commence immediately.</p>	<p>Director of Operations and Neighbourhoods</p> <p>March 2019</p>
Management of CCTV (New)	To review the processes and procedures in place across the Council to ensure consistency of approach and compliance with	<p>A report has been discussed at Board in February and the next steps are to undertake a full review of the CCTV network to include:</p> <ul style="list-style-type: none"> Review of location and numbers of CCTV Cameras 	Director of Operations and Neighbourhoods

Area of Review	Improvement Required	Progress to Date	Improvement Owner and Completion Date
	all relevant legislative requirements.	<ul style="list-style-type: none"> Invest to Save Income Generation Service Review <p>The above actions address the issues identified in the CCTV Internal Audit Report.</p>	March 2019
Creditors (New)	Improvements to the creditor payments system have been highlighted as part of an internal audit review.	A full system review is currently underway to review the process from procurement to payment.	Director of Governance and Pensions March 2019
Estates Management (New)	Improvements to the Estates Management system have been highlighted as part of an internal audit consultancy review.	A full service review is currently underway in response to the recommendations made and as a result of the liquidation of Carillion as the service is currently outsourced. Work to consider different delivery models including a combined Estates Provision with the ICFT is to commence and be completed during 2018/19.	Director of Growth March 2019
ICT Disaster Recovery and Business Continuity Planning (New)	Enhancements are needed to the systems in place so that they meet with the requirements of the Council and best practice, to ensure continuity of service in the event of an incident, which causes disruption, or denial of service.	A meeting is scheduled for June with the AGMA Civil Contingencies and Resilience Unit to review the system in place and discuss how the unit may support the Strategic Commission to improve business continuity across all services.	Director of Finance October 2018
Information Governance (New)	To ensure that information governance processes across the Council are consistently applied and compliant with the EU General Data Protection Regulations and the new Data Protection Act 2018.	<p>An action plan is in place and monitored by the Information governance Group to ensure that the Council is compliant with the new regulations and legislation.</p> <p>An additional post has been added to the Risk and Insurance Team and once recruitment is complete, it will provide extra capacity to this critical agenda.</p>	<p>Director of Governance and Pensions</p> <p>Director of Finance</p> <p>September 2018</p>

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officer:	Wendy Poole – Head of Risk Management and Audit Services
Subject:	RISK MANAGEMENT AND AUDIT SERVICES PLANNED WORK 2018/19
Report Summary:	This report presents the planned work for the Risk Management and Audit Service for 2018/19.
Recommendations:	<ol style="list-style-type: none">1. Members approve the Draft Internal Audit Plan for 2018/19 shown at Appendix 1 and note the planned work for the Risk Management and Insurance Team and the National Anti-Fraud Network.2. Members approve the Quality Assurance and Improvement Programme for 2018/19 shown at Appendix 2.
Links to Community Strategy:	Internal Audit supports the individual operations, which deliver the objectives within the Community Strategy.
Policy Implications:	Effective Internal Audit and Risk Management supports the achievement of Council objectives and demonstrates a commitment to high standards of corporate governance.
Financial Implications: (Authorised by the Section 151 Officer)	Effective Internal Audit assists in safeguarding assets, ensuring the best use of resources and reducing losses due to poor risk management. It also helps to keep insurance premiums to a minimum and provides assurance that a sound control environment is in place.
Legal Implications: (Authorised by the Borough Solicitor)	Demonstrates compliance with the Accounts and Audit Regulations 2015.
Risk Management:	By assisting in the effective management of risks, Internal Audit helps to reduce costs and improve service delivery.
Access to Information:	The background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by:  Telephone: 0161 342 3846  e-mail: wendy.poole@tameside.gov.uk

1. INTRODUCTION

- 1.1 The report presents the planned work for the Risk Management and Audit Service for 2018/19. It sets out in detail the work of Internal Audit and presents at **Appendix 1** the Annual Audit Plan for 2018/19 for approval. It highlights the planned work in relation to Counter Fraud/Investigation Work, the Risk Management and Insurance Team and the National Anti-Fraud Network (NAFN) – Data and Intelligence Services.

2. INTERNAL AUDIT PLANNING PROCESS

- 2.1 The Internal Audit Service plans its work with a view to achieving the following key objectives:
- Supporting the Council's Vision;
 - Providing optimum coverage across all services to ensure the best use of resources;
 - Targeting resources towards priority (high-risk) areas;
 - Satisfying legislative requirements;
 - Providing assurances to Members and Senior Managers as to the effectiveness of the Council's internal controls;
 - Responding to the needs of service managers; and
 - Maintaining a regular level of audit presence in all areas.
- 2.2 The plan is reviewed and revised each year to take into account service and legislative changes, which can result in large shifts in priorities and culminates in the production of the Annual Audit Plan.
- 2.3 The audit management system used ("Galileo") holds the entire list of all audits to be undertaken "the Audit Universe" and this is used as part of the consultation process.
- 2.4 Audits are prioritised based on an assessment of risk and allocated a numerical risk score which equates to either High, Medium/High, Medium, Low/Medium or Low and the following factors are taken into account:-
- Susceptibility to Error/Fraud;
 - Control Environment;
 - Sensitivity and Reputation of the Council;
 - Complexity;
 - Volume and Value of Transactions;
 - Management Concerns;
 - Management Changes;
 - Specific Business Risks/Business Importance;
 - Quality, Integrity and Security of Information; and
 - Years since Previous Audit.
- 2.5 Consultation involves Executive Members, Executive Directors, Assistant Directors, Heads of Service and in some cases Service Unit Managers and was carried out during March. These meetings help to inform the risk assessments undertaken on audit activities and provide members and officers with the opportunity to discuss areas of concern or provide further details of up and coming changes to structures, key personnel, systems, procedures and/or legislation. In addition to agreeing priority audits, the discussions also include a report on previous audit work undertaken and the level and quality of the service provided. Risks identified in the Corporate Risk Register and other sources of assurance across the Council are also taken into account during the planning process.
- 2.6 Allegations of fraud investigated during the year together with intelligence gained from external sources (e.g. Chartered Institute of Public Finance and Accountancy Fraud Centre,

National Anti-Fraud Network and networking events) are used to identify potential risks and new fraud areas which are then taken into account either directly as an audit or used to inform the audit work scheduled in a particular area.

- 2.7 Taking all the above information into account, the draft plan is produced. This plan is then balanced to resources and priorities and amended accordingly, as requested audits usually exceed resources available. This stage of the process is conducted by the Head of Risk Management and Audit Services supported by the Principal Auditors who manage the plans on a day-to-day basis and is based on professional judgement and the potential risk exposure posed to the Council. Audits that cannot be covered in the current plan year are highlighted as priorities for next year's audit plan and held in contingency in case difficulties arise in achieving any of the audits included in the annual plan.
- 2.8 The Director of Finance (Section 151 Officer) and the Assistant Director of Finance have been consulted to ensure that the levels of coverage will provide the necessary information and assurance to support the Section 151 Officer Role and the preparation of the Annual Governance Statement.
- 2.9 Whilst the work of Internal Audit, External Audit and Scrutiny are different, consultation takes place during the year to ensure our respective work programmes are complementary and that areas are not "over audited/inspected".

3. INTERNAL AUDIT ANNUAL AUDIT PLAN 2018/19

- 3.1 A summary of the Annual Audit Plan is shown below in Table 1.

Table 1 – Annual Audit Plan Summary 2018/19

Service Area / Directorate	Planned Days	%
Children's	89	5.0
Children's Schools/Learning	243	14.0
Adults	102	6.0
Population Health	25	1.5
Growth	71	4.0
Operations and Neighbourhoods	106	6.0
Governance	164	9.0
Finance and ICT	174	10.0
Greater Manchester Pension Fund	300	17.0
Cross Cutting	20	1.0
Counter Fraud Work and Investigations	463	26.5
Total Planned Days for 2018/19	1,757	100.0

- 3.2 A complete list of the Annual Audit Plan for 2018/2019 is included at **Appendix 1**. The detail contained in the plan has been expanded in response to the recent Peer Review Assessment and now covers:-
- Links to the Corporate Plan (New);
 - Links to the Corporate Risk Register (New);
 - Auditable Area;
 - Purpose of the Audit;
 - Priority (New);

- Audit Category (New); and
- Planned Days for 2018/19.

3.3 The new additional columns in the plan are explained in further detail below:-

- **Links to the Corporate Plan**
Each audit in the plan has been linked to one of the five themes within the Corporate Plan with the additional of a sixth theme to cover Governance and Finance, as outlined in the table 2 below.

Table 2 – Corporate Plan Themes

Excellent Health and Care	We want all our residents to have access to high quality joined up health and care services that help our residents to live longer and healthier lives.
Successful Futures	We want our young people to live in a safe and supportive environment where they have the opportunity to reach their full potential.
Vibrant Economy	We want to provide greater access to jobs and opportunities, attract more businesses to the area and improve connectivity.
Stronger communities	We want to build stronger communities that look out for one another, take pride in the area they live in and have access to quality homes.
Digital Place	We want to provide everyone with the opportunity to get on-line to access services, learning and information.
Governance and Finance	To provide support to the Council in delivering its aims and objectives.

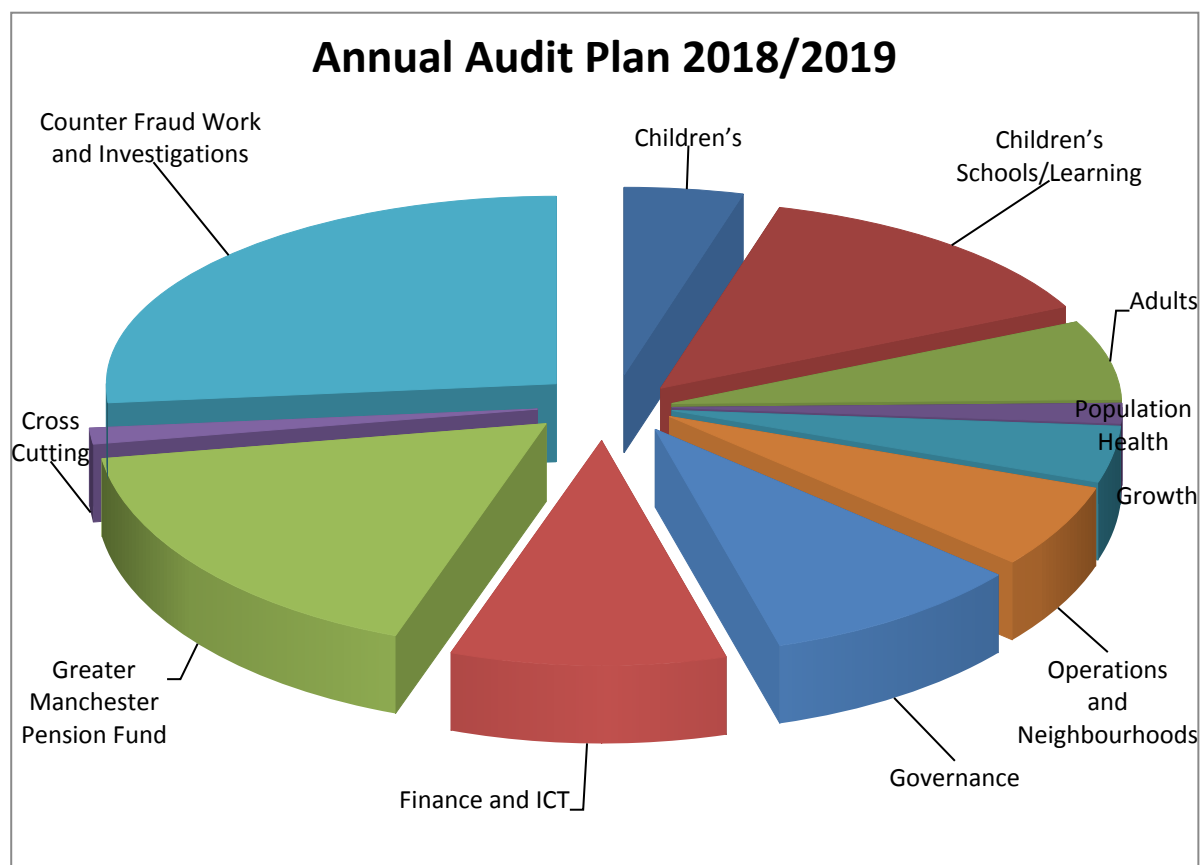
- **Links to the Corporate Risk Register**
Where appropriate each audit has been linked a risk in the Corporate Risk Register to ensure that the plan is providing audit coverage in the areas deemed to be of significant risk to the Council.
- **Priority**
Two categories have been included;
 - Mandatory – Audits/Audit Processes that need to be included e.g. grant certification work.
 - High/Medium/Low – Each audit in the ‘Audit Universe’ is risk assessed within the audit management system ‘Galileo’ and allocated a numerical score. Those with the highest scores are included in the plan until all available resources have been accounted for.
- **Audit Category**
The audit categories included in the plan are detailed below in table 3.

Category	Description
Assurance	To provide assurance to management that the processes in place are robust and fit for purpose.
Risk Based	A comprehensive risk based audit review is undertaken.
Financial Control/ Assurance Testing	A programme of financial system reviews considered high risk.
Advice	Ongoing advice provided at the request of management and stakeholders.

Follow Up	Work undertaken to ensure recommendations documented in Final Reports have been implemented.
School Visits	A programme of school visits identified as highest risk taking into account any key changes in personnel, systems and finances
Investigation	Ad hoc investigations into suspected fraud, irregularities and information incidents.
Computer Audit	Commissioned audit reviews of a technical nature from Salford Computer Audit Services, combined with reviews to be delivered in-house.
Contract Audit	Reviews on specific procurement activities and contracts considered high risk.
Certification Work	Independent verification work required by grant funding bodies, legislation and Final Accounts certification.

- 3.4 The plan detailed at **Appendix 1** and summarised in the table above and the pie chart below totals 1,757 days and has been matched to available resources. Compared to the plan for 2017/18 the available days have increased by 91 days from 1,666 as all posts within the Internal Audit Team are now occupied.
- 3.5 Productive days are estimated and any changes to the assumptions made will be reflected during the year as Audit Plan updates and reported to the Audit Panel.
- 3.6 The plan will be kept under constant review and regular meetings will be held with Executive Members and the Senior Management Team to ensure that it reflects the keys risks for the Council going forward as it continues to change both in shape and size to meet the financial challenges placed upon it.

Pie Chart 1 – Annual Audit Plan 2018/2019



4. INTERNAL AUDIT STAFFING

4.1 The structure of the team is shown in Table 2 below.

Table 2 – Internal Audit Staffing Structure

Post	Qualification	Audit Experience
Head of Risk Management and Audit Services	CIPFA/PGCM	Over 20 Years
Principal Auditor	CIPFA/PGCM	Over 20 Years
Principal Auditor	ACCA/IIA	Over 20 Years
Senior Auditor	CIPFA	Over 20 Years
Senior Auditor		Over 20 Years
Senior Auditor		Over 20 Years
Counter Fraud/Investigator	CIPFA ACFTech	Over 10 Years
Counter Fraud/Investigator	CIPFA ACFTech	Less than 1 Year
Auditor	Degree	2 – 5 Years
Auditor	Degree	Less than 1 Year

4.2 The Service Unit no longer employs a specialist Computer Auditor and therefore the provision of technical computer audit support is procured from Salford MBC Computer Audit Services using the AGMA Collaboration Computer Audit Agreement to help deliver the ICT – Computer Audit Plan.

4.3 The Internal Audit Team has complete organisational independence and is not responsible for any non-audit work. Staff are very aware of the need to remain independent and ensure that requests for advice and support do not compromise this position.

- 4.4 The Head of Risk Management and Audit Services is responsible for the Risk Management and Insurance functions and is the Council's Senior Information Risk Owner (SIRO), which does challenge her independence. Any review conducted in these areas would be reported in the name of an independent manager namely the Assistant Director of Finance (Deputy Director of Finance) to ensure that independence is not compromised.
- 4.5 All members of the Internal Audit Team sign an annual declaration form, and this includes confirming that they have read and agreed to adhere to the Tameside Code of Conduct for Employees and the Public Sector Internal Audit Standards - Code of Ethics.

5. INTERNAL AUDIT REPORTING PROCESS

- 5.1 At the completion of an audit review a draft report is produced which is issued to the appropriate managers within the area (this will vary depending on the review, but usually includes members of the senior management team) for them to check the factual accuracy of the report and to provide their management responses to the recommendations identified. Closure meetings are held with all parties to expedite the process.
- 5.2 A quality control and review process is in place within the team that ensures all audits are conducted to a high standard and that working papers, conclusions and recommendations are sound and justified.
- 5.3 A final audit report is then produced incorporating the management responses and circulated to: -
- Executive Member – responsible for area under review;
 - Chief Executive;
 - Director of Governance and Pensions (Monitoring Officer);
 - Director of Finance (Section 151 Officer);
 - Assistant Director of Finance (Deputy Section 151 Officer);
 - Director;
 - Appropriate Service Area Managers;
 - Financial Management Business Partner; and
 - External Audit.
- 5.4 Six months after completion, a Post Audit Review is undertaken to establish whether the agreed recommendations have been implemented, however where a low level of assurance is issued the area is re-visited within 3 months. This report is circulated to those members and officers who received the final report so that they can check that progress has been made. Areas of concern are escalated to the Head of Risk Management and Audit Services and/or the Director/Assistant Director of Finance for discussion with the relevant service managers to ensure that progress is made. Post Audit Reviews with significant outstanding items will in turn be reported to the Audit Panel.
- 5.5 All reports issued are reviewed and quality checked within the team by the Principal Auditors before they are released. The Head of Risk Management and Audit Services also reviews all Final Reports and Post Audit Reviews. Low level assurance audits are discussed with Assistant Directors to gain assurance that resources will be targeted to resolve issues identified.
- 5.6 In addition, quarterly reports are produced for the Audit Panel, which summarise the key issues, highlighted from completed audits and any concerns resulting from Post Audit Reviews.
- 5.7 At the end of the financial year, an annual report is produced summarising the work undertaken during the year and providing an opinion on the overall control environment. In

broad terms, the opinion is based on the audit opinions issued during the year, the nature of the audits and the type and severity of recommendations made.

- 5.8 The Internal Audit service conforms with the Public Sector Internal Audit Standards, and this was confirmed in the report received in April 2018 following the External Peer Review Assessment in March 2018 and this informs the Review of the Effectiveness of the System of Internal Control required by the Accounts and Audit Regulations 2015 Section 6.
- 5.9 A self-assessment against the Chartered Institute of Public Finance and Accountancy Statement for the Head of Internal Audit has also been completed as part of the Review of the Effectiveness of the System of Internal Control and as part of the assurance work for the preparation of the Annual Governance Statement. The Head of Risk Management and Audit Services is compliant with all the requirements.

6. ANNUAL GOVERNANCE STATEMENT

- 6.1 The Accounts and Audit Regulations 2015 require audited bodies to conduct a review, at least once a year, of the effectiveness of its systems of internal control. The findings of the review shall be considered by a committee of the relevant body, or by members of the relevant body meeting as a whole, and following consideration, shall approve a governance statement, prepared in accordance with proper practices in relation to internal control.
- 6.2 The work of Internal Audit is fundamental to the production of this statement as the work conducted provides evidence and ongoing assurance that the systems of internal control have been reviewed and that risks are being effectively managed. The annual report referred to in 5.7 is a key source of assurance.

7. INTERNAL AUDIT CHARTER

- 7.1 The Internal Audit Charter was approved by the audit Panel on 6 March 2018. In terms of feedback from the External Peer Review, the revised charter met all the required standards and no recommendations were received in this area.

8. QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME

- 8.1 Standard 1300 of the Public Sector Internal Audit Standards require:
"That the chief internal auditor must develop and maintain a quality assurance and improvement programme that covers all aspects of the internal audit activity".
- 8.2 The Quality Assurance and Improvement Programme (attached at **Appendix 2**) includes:-
- Introduction;
 - Internal Assessments;
 - External Assessments;
 - Service Development; and
 - Review of the Quality Assurance and Improvement Programme.
- 8.3 The format of the Quality Assurance and Improvement Programme has been amended for 2018/19 to include a section on service development as this was highlighted as part of the External Peer Review and the following recommendation made:-
"A Quality Assurance and Improvement Programme (QAIP) is in place which is updated on an annual basis and presented to Audit Panel in line with the standards. It was noted that no improvement action plan was linked to this to highlight what actions had been identified to drive improvement and enable the Audit Panel to monitor the achievement of these"

9. PROACTIVE FRAUD WORK/IRREGULARITY INVESTIGATIONS

- 9.1 Whilst unplanned in their nature, time is required each year for the investigation of frauds and irregularities that are notified to Internal Audit. There is a dedicated resource within the service unit, which provides support to management to ensure that such problems are dealt with as effectively as possible. A control report is provided in response to investigations/advice and support work to ensure that the control environment is improved to try to minimise any future re-occurrence. Learning points are noted for wider dissemination where appropriate and any recommendations are followed up at a later date by a Post Audit Review to ensure the required improvements have been implemented.
- 9.2 The Standards Panel is notified of all cases reported and kept informed of progress on a monthly basis and direction/guidance from the Panel is provided where appropriate.
- 9.3 Update reports will be provided as part of the quarterly progress reports provided by the Head of Risk Management and Audit Services.
- 9.4 Intelligence from all corporate fraud/irregularities notified to Internal Audit is used to:-
- Evaluate our response plan;
 - Inform the audit planning process to ensure fraud risks are taken into account; and
 - Inform the risk assessment tool within Galileo (audit management system) to ensure all auditable activities are correctly assessed.
- 9.5 Proactive fraud work planned for 2018/2019 will include the development and delivery of awareness training, the review of all fraud policies, processes and procedures and the use of the interrogation package "IDEA" to look for data anomalies and duplicate payments.

10. RISK MANAGEMENT AND INSURANCE

- 10.1 The Risk Management and Insurance Team provide services to the whole Council including schools. The key priorities for the team during 2018/2019 are:-
- To review the risk management system to ensure that it complies with best practice including a review of service area risk register.
 - To ensure the Corporate Risk Register is updated on a quarterly basis and reported to the Single leadership Team and the Audit Panel.
 - To facilitate the continued implementation of the Information Governance Framework, ensuring that the Council is compliant with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.
 - To review the Business Continuity Management system in place to streamline the process to create a management tool that is workable, with the capability to provide knowledge and information should a major incident occur affecting service delivery.
 - To review the insurance database used by the team to ensure it is fit for purpose and that the reporting function is efficient and effective.
 - To continue to support managers to assess their risks as services are redesigned to ensure that changes to systems and procedures remain robust and resilient offering cost effective mitigation and that claims for compensation can be successfully repudiated and defended should litigation occur.
 - To attend management team meetings quarterly to provide updates on insurance, information governance, risk management and business continuity.

11. NATIONAL ANTI-FRAUD NETWORK - DATA AND INTELLIGENCE SERVICES

11.1 The National Anti-Fraud Network will continue to work with key stakeholders and partners to further develop the services offered to members to ensure that emerging business needs are met in response to changing legislation. The key priorities are:-

- To continue to maintain and where necessary improve operational controls in pursuit of operational excellence to meet Government standards on data and intelligence.
- To work with the Investigatory Powers Commissioner's Office (IPCO) to maintain high standards of integrity and legitimate use for communications data and ensure compliance with the Investigatory Powers Act once enacted.
- To improve the website, taking on board customer feedback and providing a more intuitive efficient experience.
- To enhance the current national sanctions database include data from service areas such as tenancy, blue badge and employee fraud.
- To engage proactively with existing data providers including Callcredit, Equifax, GB Group and Lexis Nexis to further expand Type B online services.
- To continue to develop DVLA services for new and existing members and explore opportunities for acquiring and linking to new data sources to expand intelligence and support fraud investigation.
- The new Taxis Licence and Revocation Database will be operational by May 2018 but will need to be actively promoted and rolled out to NAFN users. During 2018/19 access to the Automatic Number Plate Recognition (ANPR) system will be introduced as a new service for members and it is anticipated that a decision on a preferred business solution for the Greater Manchester Intel Hub will lead to implementation.
- To pursue the updated strategy approved by the Executive Board in January 2018 to develop training and the provision of an intelligence analyst service, by seeking stakeholder and member support and scoping out the revised service offering.

12. PERFORMANCE MONITORING

12.1 In accordance with Tameside methodology, the performance of the service is monitored against targets and performance indicators. Individually auditors are monitored against performance targets and appraisal sheets are completed for audits highlighting issues and potential training needs. Customer questionnaires are also used at the conclusion of each audit to test customer reaction to the audit and to help identify any training needs or service improvements.

12.2 The Audit Plan will be continually monitored via monthly progress meetings between the Audit Management Team and regular update meetings with Executive Members, Senior Managers and External Audit and quarterly reports to the Audit Panel and the Greater Manchester Pension Fund Local Board.

12.3 The target for achievement is 90% of the agreed plan. However, high priority requests that arise during the year, changes in available audit resources and problem areas highlighted may affect the achievement of this target and result in the need for revisions to the agreed plan. All significant changes are agreed with relevant managers and Executive Members where appropriate and will be brought to the Panel for approval.

12.4 The Public Sector Internal Audit Standards are the benchmark against which the performance and effectiveness of the internal audit service will be measured.

12.5 The performance indicators monitored and measured are detailed in table 3 below.

Table 3 – Performance Indicators

	INDICATOR	TARGET
1	Compliance with Public Sector Internal Audit Standards	100%
2	% of Plan Completed	90%
3	Customer Satisfaction (per questionnaires)	90% of customers “satisfied ≥ 65%”
4	% Recommendations Implemented	90%
5	No. of Irregularities Reported/Investigated	Downward Trend

13. MEMBER TRAINING

- 13.1 During the year, general training on Audit, Risk Management, Information Security, Corporate Governance and Business Continuity will be considered in accordance with member needs with targeted training being provided for members of the Audit Panel and the Greater Manchester Pension Fund Local Board as and when requested.

14. RECOMMENDATIONS

- 14.1 Members approve the Draft Internal Audit Plan for 2018/2019 shown at **Appendix 1** and note the planned work for the Risk Management and Insurance Team and the National Anti- Fraud Network.
- 14.2 Members approve the Quality Assurance and Improvement Programme for 2018/19 shown at **Appendix 2**.

This page is intentionally left blank

DRAFT INTERNAL AUDIT PLAN 2018/19

APPENDIX 1

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
CHILDRENS						
Successful Futures	CR 7	Troubled Families	An allocation has been included to carry out checks on the Troubled Families Scheme in accordance with a GM wide audit programme.	Mandatory	Assurance	10.0
	CR 6	Childrens Homes	To review the financial, health and safety and risk assessment procedures at the Homes in addition to ensuring that the outcomes for the children are achieved.	High	Risk Based	20.0
	CR 6	Emergency/Cash Payments	A review will take place of the cash/emergency payments being made by Childrens Services to ensure robust processes are in place.	High	Risk Based	10.0
	CR 6	Liquid Logic	To review the system to ensure the security, technological and access controls are robust to protect the sensitive information within the system.	High	Risk Based	10.0
	CR 14	Budgetary Control and Financial Management	To review the processes for monitoring the budget within Childrens Services	High	Financial Control Assurance Testing	15.0
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	6.0
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	3.0
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	10.0
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	5.0
TOTAL PLANNED DAYS FOR CHILDRENS						89
CHILDRENS - SCHOOLS/LEARNING						
Successful Futures	CR 20	Gorse Hall Primary & Nursery School	To review the Financial Management/ICT Procedures/Information Governance Procedures of the school to ensure robust processes and procedures are in place in accordance with best practice to deliver a strong control environment.	High	School Visits	6
		Stalyhill Junior School				6
		Stalyhill Infants School				6
		Buckton Vale Primary School				6
		Lyndhurst Primary & Nursery School				6
		Ravensfield Primary School				6
		Broadbottom CE Primary School				6
		Mottram CE Primary School				6
		St Johns CE Primary School				6
		Micklehurst Primary School				6
		Holy Trinity CE Primary				6
		St Marys CE Infant & Nursery School Droylsden				6
		St Josephs RC Primary & Nursery School				6
		St John Fisher RC Primary School				6
		St Christophers RC Primary School				6
		Samuel Laycock School				6
		Mossley Hollins High School				10
		St Damians RC Science College				10
		St Thomas More RC College				10
		Cromwell High School				10

DRAFT INTERNAL AUDIT PLAN 2018/19**APPENDIX 1**

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
	CR 12	Payroll - Schools, incl Third Party Providers	To ensure that there are adequate controls in place, and the payroll rules are being complied with re payroll in schools, including where the service has been outsourced.	High	Risk Based	15
	CR 6	Special Educational Needs and Disability (SEND)	A review of the service provided and the financial allocation of funding.	High	Risk Based	15
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	8
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes. Provision of School Newsletter.	Mandatory	Advice	15
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	40
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	14
TOTAL PLANNED DAYS FOR SCHOOLS/LEARNING						243

ADULTS						
Excellent Health and Care	CR 4	Integrated Urgent Care Team	To provide assurance that effective internal controls are in place in respect of the Integrated Urgent Care Team.	High	Risk Based	15
	CR 4	Locality Teams - Care Management	To provide assurance that effective internal controls are in place in respect of Care Management.	High	Risk Based	15
	CR 3	Nursing and Residential Home Placements-Payments	To provide assurance that effective internal controls are in operation in respect of the placement of clients into residential/nursing homes and that the payments made are correct.	High	Risk Based	15
	CR 10	Shared Lives	To review the processes in place for the delivery of the Shared Lives Service.	High	Risk Based	15
	CR 14	Budgetary Control & Financial Management	To ensure effective arrangements are in place in respect of Budgetary Control and Financial Management.	High	Financial Control Assurance Testing	15
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	8
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	10
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	7
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	2
TOTAL PLANNED DAYS FOR ADULTS						102

POPULATION HEALTH						
Excellent Health and Care	CR 8	Disabled Facilities Grant	Certification to confirm that expenditure has been incurred in accordance with the grant conditions.	High	Certification Work	3
	CR 8	Health and Wellbeing - Health Visiting Service	To review the process in place for the commissioning and monitoring of the Health Visiting Service as an aspect of the Mandatory Healthy Child Programme (0-5).	High	Risk Based	15
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	3

DRAFT INTERNAL AUDIT PLAN 2018/19**APPENDIX 1**

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	1
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	2
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High		1
TOTAL PLANNED DAYS FOR POPULATION HEALTH						25

GROWTH						
Vibrant Economy	CR 12	Inspired Spaces - Monitoring Of The Catering Contract	To provide assurance that effective contract monitoring processes are in place in order to ensure compliance.	High	Contract Audit	15
	CR 22	Estate Acquisitions and Disposals	To provide assurance that the Council's Estate is being effectively managed and appropriate governance is in place in respect of acquisitions and disposals.	High	Risk Based	15
	CR 2 CR 5	Vision Tameside	To provide assurance that effective processes are in place in order to deliver the project within the revised timeframe and within budget.	High	Contract Audit	15
	CR 17	Planning Process	To provide assurance that effective systems are in place in respect of the planning process.	High	Risk Based	15
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	4
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	1
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	6
TOTAL PLANNED DAYS FOR GROWTH						71

OPERATIONS AND NEIGHBOURHOODS						
Stronger Communities		Transport	To provide assurance that effective internal controls are in place in respect of the provision of transport.	High	Risk Based	15
	CR 30	Youth Service	To ensure effective internal controls are in place in relation to the delivery of the Youth Service.	High	Risk Based	15
	CR 6 CR 10	Provision of the Integrated Transport Service	To provide assurance that internal controls are in place to ensure the effective provision of transport to service users.	High	Risk Based	20
		Servitor	To review the process for calculating engineering recharges to ensure that they are being correctly determined.	High	Computer Audit	15
	CR 14	Local Authority Bus Subsidy Grant	Certification to confirm that expenditure has been incurred in accordance with the grant conditions.	Mandatory	Certification Work	2
		Hattersley Collaboration Agreement	To undertake an audit of the Final Accounts.	Mandatory	Certification Work	5
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	7
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	12
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	11
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	4
TOTAL PLANNED DAYS FOR OPERATIONS AND NEIGHBOURHOODS						106

GOVERNANCE

DRAFT INTERNAL AUDIT PLAN 2018/19**APPENDIX 1**

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
Successful Futures	CR 29	Softbox	A review is planned to look at the whole system from Childrens Services through to the payment on Softbox, to ensure that the controls to prevent overpayments are operating effectively.	High	Risk Based	15
Excellent Health and Care	CR 29	Determination and Recovery of Adult Service Care and Support Charges	To review the processes in place within Exchequer Services to ensure that charges are being correctly calculated and promptly recovered.	High	Risk Based	15
Governance and Finance	CR 29	Debtors Full System	To provide assurance that all invoices are correctly raised and income is promptly collected and appropriately accounted for.	High	Financial Control Assurance Testing	15
Successful Futures	CR 14	Apprenticeship Levy	A review of the processes within the organisation, including the finance process.	High	Risk Based	15
Governance and Finance	CR 29	iTRENT Self Service	We will sign off the new module to ensure that the appropriate procedure has been followed prior to the implementation and the system is fit for purpose and secure.	High	Assurance	10
Digital Place	CR 1	Social Media Controls	A review will be carried out to ensure that the set up and security of the Authority's Social Media accounts is robust and in line with recommended practice.	High	Computer Audit	5
Governance and Finance	CR 14	GMPF Annual Return - Compliance Checks	Checks on the compliance checklist submitted with the GMPF Annual Return, to enable it to be signed off by the Head of Internal Audit.	Mandatory	Certification Work	4
	CR 14	External Audit Checks - Payroll	External Audit select a sample from iTrent and Internal Audit carry out checks and provide the evidence to support the transactions. External Audit rely on this work to obtain assurance that the payroll system is operating effectively.	Mandatory	Financial Control Assurance Testing	6
	CR 29	Registrars Financial Audit	An allocation is included in the Plan each year to review the records and income in respect of individual Registrars, on a cyclical basis.	Mandatory	Assurance	6
	CR 14	Members Allowances - Publication	To provide data assurance in relation to the publication of members allowances.	Mandatory	Assurance	3
	CR 29	Review of Financial Regulations	To review and make recommendations to update Financial Regulations.	Mandatory		2
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	8
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	30
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	16
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	14
TOTAL PLANNED DAYS FOR GOVERNANCE						164

FINANCE AND ICT						
Governance and Finance	CR 24	Insurance	To review the arrangements in place for the delivery of the insurance function.	High	Risk Based	15
	CR 12	Procurement	Contingency days to be discussed with Director of Finance and Assistant Director of Finance to review procurement processes.	High	Risk Based	15
	CR 13	Information Governance	A review of the arrangements in place in respect of Information Governance.	High	Risk Based	15
	CR 29	Risk Management	A review of the arrangements in place in respect of Risk Management.	High	Risk Based	15
	CR 29	Bank Reconciliation Procedures	To provide assurance that bank reconciliations are being correctly undertaken on a regular/timely basis and that any discrepancies are being promptly investigated.	High	Financial Control Assurance Testing	10

DRAFT INTERNAL AUDIT PLAN 2018/19**APPENDIX 1**

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
Digital Place	CR 1	Cyber Security Review	The review will examine the controls in place, to ensure that the Authority is protected from cyber attacks.	High	Computer Audit	15
	CR 1	Network Security (incl 3rd Party access)	The review will examine the controls in place to secure the Network and will include the controls to enable authorised third parties to access the network.	High	Computer Audit	10
	CR 1	ISO 27001 Gap Analysis	Although the Authority does not have this formal accreditation, it is planned to compare the recommended controls in the Standard to the controls that are currently in place.	High	Computer Audit	10
	CR1	ICT Recharges	A review is planned to examine the determination and accounting of the recharges.	High	Risk Based	15
Governance and Finance	CR 14	External Audit Checks - General Expenditure	To undertake checks on a sample of expenditure transactions to ensure that they are appropriate to the needs of the Council, have been appropriately authorised and correctly accounted for. This task is undertaken on behalf of External Audit and the results are used to inform the Audit of the Final Accounts.	Mandatory	Financial Control Assurance Testing	6
	CR 12	Click Travel	To provide assurance that effective arrangements are in place in respect of procuring travel and accommodation arrangements.	High	Risk Based	15
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	8
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	10
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	11
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	4
TOTAL PLANNED DAYS FOR FINANCE AND ICT						174
GREATER MANCHESTER PENSION FUND						
Vibrant Economy	CR 27	Northern Pool	A review will take place of the Governance arrangements for the newly formed Northern Pool.	High	Risk Based	15
	CR 27	GLIL Regulated vehicle	A review will take place of the systems and procedures within GLIL in respect of the investments that are currently active.	High	Risk Based	10
Governance and Finance		Compliance Function	A review is planned of the Compliance function to ensure that appropriate Compliance procedures have been put in place.	High	Risk Based	15
	CR26	First Bus Asset Transfers	A check will be made to ensure that the transfer of assets in relation to the First Bus pension liabilities has been carried out correctly.	High	Assurance	10
	CR26	Transfer of Assets re Capital International	Checks will be carried out to ensure the accuracy and completeness of the asset transfers in relation to the previous Fund Manager.	High	Assurance	10
	CR26	Transfer of Assets to new Custodian	Checks will be carried out to ensure the accuracy and completeness of the asset transfers between the old and new custodian.	High	Assurance	10
Vibrant Economy	CR27	Pooled Private Equity Vehicle	A review will be carried out of the systems in place in relation to the Pooled Private Equity Vehicle.	High	Risk Based	15
Digital Place	CR 13	iConnect	We will sign off this new module of Altair, prior to it going live, to ensure the system is fit for purpose and secure.	High	Assurance	5
Governance and Finance		Altair - Administration to Payroll Upgrade	The Payroll module of Altair is being upgraded to Java and Internal Audit have been asked to perform some data checks prior to the new upgrade going live.	High	Assurance	5
		Benchmarking-KPI's	A review will take place of the Pension Funds Benchmarking and Performance Indicators.	High	Assurance	10

DRAFT INTERNAL AUDIT PLAN 2018/19**APPENDIX 1**

LINK TO CORPORATE PLAN	LINK TO RISK REGISTER	AUDITABLE AREA	PURPOSE OF AUDIT	PRIORITY	AUDIT CATEGORY	PLANNED DAYS 2018/19
Finance	CR 29	Segregation of Duties - New Structure	To ensure that segregation of duties is not compromised by the new staffing structure.	High	Risk Based	5
		Move to Barclays Bank	A review will be carried out on the system/process followed for the Private Equity Investments.	High	Assurance	5
Digital Place		Member Self Service	We will sign off this new module of Altair, prior to it going live, to ensure the system is fit for purpose and secure..	High	Assurance	10
Governance and Finance		Move from Citrix re Altair	We will sign off this new module of Altair, prior to it going live, to ensure the system is fit for purpose and secure..	High	Assurance	5
		Visits to Contributing Bodies	An allocation of days is included annually for Internal Audit to carry out visits to a sample of Employers. The auditor reviews the data held on the Employer's payroll system to ensure that the correct contributions are being paid over to the Pension Fund.	Mandatory	Employer Visits Compliance Testing	70
		Contribution Income (including processing of Year End returns)	Contribution Income is reviewed annually, as it is the main income of the Pension Fund, paid over to the Fund by Employers. External Audit rely on our work on this area, to ensure that there are processes in place to monitor and review the contributions received.	Mandatory	Financial Control Assurance Testing	15
	CR13	Information Governance/Security Incidences	Investigation of Information Security Breaches under the Information Security Incident Reporting Procedure/Practice Note.	High	Investigation	10
		Planning and Control	Provision of days for planning/controlling the plan including activity reporting, meetings with Senior Management and Executive Members to ensure that changes throughout the year are reflected in the plan where appropriate.	Mandatory	-	15
		Advice and Support	Provision of days to support management in the development and maintenance of effective controls in light of new risk exposures and service changes.	Mandatory	Advice	10
		Post Audit Reviews	Follow up work to ensure audit recommendations have been implemented.	Mandatory	Follow Up	15
		Days required to complete 2017/18 Work	Days required to finalise audits that were in progress at the year end.	High	-	35
TOTAL PLANNED DAYS FOR PENSION FUND						300
CROSS-CUTTING						
Stronger Communities	CR 9	Contingency for GM Combined Authority - Devolution Assurance and Joint Working	Work programme to be determined by the Greater Manchester Combined Authority in relation to grant certification work.	Mandatory	Certification work	10
Governance and Finance	CR 13	UK Mail Advice and Support	Advice in respect of the checks that need to be undertaken by Service Areas across the Council prior to them using UK Mail.	High	Assurance	10
TOTAL PLANNED DAYS FOR CROSS-CUTTING						20

TAMESIDE MBC

INTERNAL AUDIT

DRAFT

QUALITY ASSURANCE

AND IMPROVEMENT

PROGRAMME

2018/19

CONTENTS

	Page
1. Introduction	3
2. Internal Assessments	3
3. External Assessments	4
4. Service Developments	5
5. Review of the Quality Assurance and Improvement Programme	5
6. Appendices	
A. Internal Audit Quality Control Checklist	6
B. Customer Satisfaction Questionnaire	14
C. Internal Performance Targets	15
D. PSIAS Peer Review Action Plan	16

1. INTRODUCTION

- 1.1 Internal Audit's Quality Assurance and Improvement Programme is designed to provide reasonable assurance to the various stakeholders of the Internal Audit activity that Internal Audit:
- Performs its work in accordance with its Charter, which is consistent with The Public Sector Internal Audit Standards definition of Internal Auditing and Code of Ethics;
 - Operates in an effective and efficient manner; and
 - Is perceived by stakeholders as adding value and improving Internal Audit's operations.
- 1.2 Internal Audit's Quality Assurance and Improvement Programme covers all aspects of the Internal Audit activity in accordance with the Public Sector Internal Audit Standards, Standard 1300 (Quality Assurance and Improvement Programme), including:
- Monitoring the Internal Audit activity to ensure it operates in an effective and efficient manner;
 - Ensuring compliance with the Public Sector Internal Audit Standards definition of Internal Auditing and Code of Ethics;
 - Helping the Internal Audit activity add value and improve organisational operations;
 - Undertaking both periodic and on-going internal assessments; and
 - Commissioning an external assessment at least once every five years, the results of which are communicated to the Audit Panel and the Greater Manchester Pension Fund Local Board in accordance with Standard 1312.
- 1.3 The Head of Risk Management and Audit Services is ultimately responsible for the Quality Assurance and Improvement Programme, which covers all types of Internal Audit activities, including consulting.

2. INTERNAL ASSESSMENTS

- 2.1 In accordance with PSIAS Standard 1300, internal assessments are undertaken through both on-going and periodic reviews.

On-going Reviews

- 2.2 Continual assessments are conducted through:
- Management supervision of all engagements;
 - Structured, documented review of working papers and draft reports by Internal Audit management;
 - Audit Policies and Procedures used for each engagement to ensure consistency, quality and compliance with appropriate planning, fieldwork and reporting standards;
 - Internal Quality Control Checklist to ensure consistency of reporting and reduce administrative error (Appendix A);
 - Feedback from audit clients obtained through Customer Satisfaction Questionnaires at the closure of each engagement (Appendix B);
 - Monitoring of internal performance targets (Appendix C) and annual outturn reporting to the Audit Panel;
 - Review and approval of all final reports, recommendations and levels of assurance by the Head of Risk Management and Audit Services and Principal Auditors; and
 - Regular team briefings.

Periodic Reviews

- 2.3 Periodic assessments are designed to assess conformance with Internal Audit's Charter, the Public Sector Internal Audit Standards definition of Internal Auditing, the Code of Ethics, and the efficiency and effectiveness of Internal Audit in meeting the needs of its various stakeholders. Periodic assessments are conducted through:
- Quarterly Update Reports, presented to the Audit Panel;
 - Annual risk assessments, in accordance with the Audit Charter 2018/19 and the Audit Manual, for the preparation of annual audit plan;
 - Annual review of the Effectiveness of Internal Audit, undertaken by the Head Risk Management and Audit;
 - Annual review of compliance against the requirements of this Quality Assurance and Improvement Programme, the results of which are reported to the Audit Panel;
 - Feedback from the Director of Finance, the Assistant Director of Finance and Audit Panel to inform the annual appraisal of the Head of Internal Audit, in accordance with Standard 1100;
 - Annual Development Reviews conducted for each Internal Auditor based on the principles of the CIPFA Guidance document "The Excellent Internal Auditor" (2010) to inform the appraisal process and identify individual training and development needs.
- 2.4 Results of internal assessments will be reported to the Audit Panel annually. The Head of Risk Management and Audit will implement appropriate follow-up to any identified actions to ensure continual improvement of the service.
- 2.5 Any significant areas of non-compliance with the Public Sector Internal Audit Standards that are identified through internal assessment will be reported in the Head of Risk Management and Audit's Annual Report and used to inform the Annual Governance Statement.

3. EXTERNAL ASSESSMENTS

- 3.1 External assessments will appraise and express an opinion about Internal Audit's conformance with the Public Sector Internal Audit Standards definition of Internal Auditing and Code of Ethics and include recommendations for improvement, as appropriate.

Frequency of External Assessment

- 3.2 An external assessment will be conducted at least every five years, in accordance with the Public Sector Internal Audit Standards. A system of Peer Reviews will be undertaken across the North West Chief Audit Executive Group. The Council's Internal Audit Service was assessed in March 2018 and was judged to conform to the standards, some minor recommendations were made during the Peer Review and these are detailed in Section 4 below.

Scope of External Assessment

- 3.3 The external assessment will consist of a broad scope of coverage that includes the following elements of Internal Audit activity:
- Conformance with the *Standards*, Definition of Internal Auditing, the Code of Ethics, and Internal Audit's Charter, plans policies, procedures, practices, and any applicable legislative and regulatory requirements;
 - Integration of the Internal Audit activity into Tameside's governance framework, including the audit relationship between and among the key groups involved in the process;
 - Tools and techniques used by Internal Audit;
 - The mix of knowledge, experiences, and disciplines within the staff, including staff focus on process improvement delivered through this Quality Assurance and Improvement programme;

- A determination whether Internal Audit adds value and improves Tameside's operations.

3.4 Results of external assessments will be provided to the Director of Finance and the Assistant Director of Finance and the Audit Panel. The external assessment report will be accompanied by a written action plan in response to significant comments and recommendations identified. Any significant areas of non-compliance will be reported in the Annual Report of the Head of Risk Management and Audit and in the Annual Governance Statement.

4. SERVICE DEVELOPMENTS

4.1 A key development for 2018/19 is to review the usage of the audit management system 'Galileo' to further maximise efficiencies from the use of e-technology.

4.2 To deliver the recommendations from the PSIAS Peer Review conducted in March 2018 detailed at Appendix D.

4.3 To review all fraud, bribery and corruption policies plans etc. including the whistleblowing and money laundering policies, to ensure they are fit for purpose and then consider how to effectively deliver training and awareness.

4.4 To provide an options paper for the provision of Internal Audit going forward across the Strategic Commission.

5. REVIEW OF THE QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME

5.1 This document will be appropriately updated following any changes to the Public Sector Internal Audit Standards or Internal Audit's operating environment and will be reviewed at least on an annual basis.

QUALITY CONTROL CHECKLIST

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
1	ASSIGNMENT PLANNING		
1.1	<p>Before an audit is allocated, the Principal Auditor needs to speak to the relevant AED and ask if the audit is still relevant and whether there are any issues in the area preventing us from doing the work.</p> <p>Need to ascertain from the AED if there are any:</p> <ul style="list-style-type: none"> • Ombudsman complaints • Significant CRM complaints • Court Proceedings against the Council • HR Issues • To confirm the Executive Member <p>Principal Auditor to also check with Insurance to ensure there are no insurance issues/claims.</p>		
1.2	If any issues are highlighted, discuss further with HR/Legal to determine whether the audit should go ahead or be postponed.		
1.3	Assignment allocated to auditor(s) from Audit Plan and Galileo updated.		
1.4	Speak to key Auditee to agree the timing of the audit.		
1.5	<p>Familiarisation with audit area by reading/ reviewing:</p> <ul style="list-style-type: none"> • Business Plan/other background papers/information (Intranet) • Review previous working paper file, report and PAR if applicable and note any outstanding issues, which may impact upon the terms of reference. • CIPFA Matrices • TIS Online • Better Governance Forum 		
1.6	Meet with key auditee(s) to discuss and agree the Terms of Reference and the expected dates for the Draft Report and Closure		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
	Meeting. Request access to the relevant systems as required. Also request any data downloads/reports that could be obtained to carry out analysis and testing.		
1.7	Draft Terms of Reference for review by Principal/Senior Auditor		
1.8	Email approved Terms of Reference to: Auditee AED/ED Chief Executive (SP) Monitoring Officer (SS) Section 151 Officer (BJ) Executive Member ** AED Legal Services AED People and Workforce Development Head of Resource Management External Audit (GM) BCC to Head of Risk Management and Audit ** Check the Executive Member is still relevant and whether they have an assistant.		
1.9	Update Galileo with audit start date and the date the Terms of Reference was issued.		
2	FIELDWORK		
2.1	For each area of risk being reviewed, identify expected controls that need to be in place to manage those risks. Each risk and its expected controls need to be entered onto Galileo on the Internal Control Evaluation/Action Plan (ICEAP).		
2.2	To ascertain the actual controls in place send a copy of the ICEAP to the auditee and make an appointment to visit them to agree the actual controls.		
2.3	Record the actual controls in place as per management on the ICEAP at the meeting using your laptop where possible to reduce re-working.		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
2.4	Compare the actual controls against the expected controls.		
2.5	Where there is no control or the control is unsatisfactory, record this as a finding and make an appropriate recommendation.		
2.6	Where the control appears to be satisfactory identify your testing and complete the testing section within Galileo.		
2.7	Agree test programme and prioritisation of the tests with Principal/Senior Auditor.		
2.8	Conduct tests and record results in Galileo in the Testing sections, attaching working papers where appropriate. Use IDEA where possible to select samples and also to carry out tests.		
2.9	Monitor time closely to ensure planned days are not exceeded. Ensure you leave yourself with some contingency days to undertake follow up work needed after the Draft Report and working papers have been reviewed by Principal/Senior.		
2.10	If you think you will exceed your planned days, you need to discuss progress with your Principal/Senior to review the scope and testing plan for the audit.		
2.11	Update the ICEAP with test results in terms of concise findings and recommendations.		
2.12	Discuss findings and recommendations with key auditee(s). Do not indicate what level of assurance may be allocated at this stage, in case it is altered when it is reviewed.		
3	REPORTING		
3.1	Produce the Draft Report comprising of Executive Summary, ICEAP and appropriate audit opinion.		
3.2	Ensure all required documents in respect of		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
	the audit are scanned into Galileo and stored in the working papers section.		
3.3	Pass the completed work and Draft report to Principal/Senior Auditor for review.		
3.4	Review notes compiled by Principal/Senior Auditor and followed up by Auditor concerned.		
3.5	If any HR or legal issues have been identified as part of the audit please arrange to speak to the AED Legal Services or People and Workforce Development for clarification. The objective here is to ensure that Legal agree with the auditee and that HR can give consideration to issues highlighted as there may be wider implications.		
3.6	Auditor to start completion of the Job Appraisal Sheet.		
3.7	Send Draft Report to each Auditee via e-mail, stating that they will be contacted to arrange a closure meeting to discuss the report and obtain management responses. Inform auditee(s) that they will be expected to have prepared responses to the recommendations and completed the action plan prior to the closure meeting.		
3.8	If a LOW Level of Assurance is given ensure that the appropriate AED is sent a copy of the Draft Report.		
3.9	Update Galileo accordingly.		
3.10	Arrange Closure Meeting within two weeks (of issue date) with all auditees responsible for implementing the recommendations (Principal/Senior Auditor to attend as appropriate).		
3.11	Attend Closure Meeting. At the meeting check again with all present whether there are any: <ul style="list-style-type: none"> • Ombudsman complaints • Significant CRM complaints • Court Proceedings against the Council 		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
	<ul style="list-style-type: none"> • HR Issues • Confirm the Executive Member and/or Assistant <p>Also check again with Insurance to ensure there are no insurance issues/claims?</p>		
3.12	If there are any issues the audit must be discussed with the Head of Risk Management and Audit Services.		
3.13	Compile Final Report, incorporating management responses within the Action Plan. (Also, action to be taken by whom and by when)		
3.14	Final Report reviewed by Principal/Senior Auditor.		
3.15	If any Legal or HR implications (or references to Legal/HR) have come to light in any of the management responses these must be referred to Aileen Johnson and Tracy Brennand for clearance before the AED/ED is asked to sign off the report.		
3.16	<p>Final Report to be signed off by AED/ED – Ask AED/ED if any:</p> <ul style="list-style-type: none"> • Ombudsman complaints • Significant CRM complaints • Court Proceedings against the Council • HR Issues • To confirm the Executive Member and/or Assistant <p>Also check again with Insurance to ensure there are no insurance issues/claims?</p>		
3.17	Email Final Report to Head of Risk Management and Audit for review before it is issued. If no response is received within two weeks send a reminder email.		
3.18	<p>Once review points have been cleared email Final Report in PDF format to:</p> <p>Auditees Executive Director/Assistant Executive Director,</p>		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
	Chief Executive (SP) Monitoring Officer (SS) Section 151 Officer (BJ) Executive Member(s)/Assistant Head of Resource Management External Audit		
3.19	If the Level of Assurance is LOW email a copy of the report to Councillors Jim Fitzpatrick and Bill Fairfoull.		
3.20	Update Galileo accordingly, ensuring that the Level of assurance is entered correctly and that a copy of the Final Report is saved.		
3.21	Email Customer Questionnaire (CQ) and update Galileo accordingly. Add calendar date for follow up in two weeks.		
3.22	If CQ is not returned within two weeks of issue, chase it up and ensure receipt of completed questionnaire. Any problems should be reported to Principal/Senior Auditor.		
3.23	Enter date of receipt and CQ results into Galileo.		
3.24	Job Appraisal Sheet to be completed and discussed with Auditor.		
3.25	Ensure that Galileo has been updated, a copy of the Final Report uploaded and the Level of Assurance recorded correctly.		
3.26	Auditor to schedule the PAR in calendar for three or six months time depending on level of assurance given.		
3.27	Update the PAR Spreadsheet with details.		
3.28	Scan the completed QCC into Galileo		
4	FOLLOW UP		
4.1	Before a Post Audit Review (PAR) is allocated, the Principal Auditor needs to speak to the relevant AED and ask if the PAR is still relevant and whether there are any		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
	<p>issues in the area preventing us from doing the work.</p> <p>Need to ascertain from the AED if there are any:</p> <ul style="list-style-type: none"> • Ombudsman complaints • Significant CRM complaints • Court Proceedings against the Council • HR Issues • To confirm the Executive Member and/or Assistant <p>Principal Auditor to also check with Insurance to ensure there are no insurance issues/claims.</p>		
4.2	Principal Auditor to determine the number of days for the PAR and update Galileo accordingly.		
4.3	When allocated with a PAR issue the Post Audit Review documentation to the responsible Officers.		
4.4	Update the PAR spreadsheet.		
4.5	Arrange a meeting to discuss the PAR and obtain confirmation of what action has been taken.		
4.6	Conduct PAR, based upon information obtained/ received. Ensure that adequate testing is undertaken and evidence is obtained and uploaded on to Galileo to support implementation of the recommendation(s).		
4.7	Compile PAR, incorporating management responses and Internal Audit Findings.		
4.8	PAR reviewed by Principal/Senior Auditor.		
4.9	If any Legal or HR implications (or references to Legal/HR) have come to light these must be referred to Aileen Johnson and Tracy Brennand for clearance before the AED/ED is asked to clear the report.		

QUALITY CONTROL CHECKLIST – NON SCHOOL AUDITS			
No.	Task	AUDITOR INITIALS/DATE	SUPERVISOR INITIALS/DATE
4.10	Obtain sign-off from AED/ED - Ask AED/ED if any complaints, ombudsman complaints or HR issues are ongoing which may be affected if the PAR were to be issued.		
4.11	Email a copy of PAR to the Head of Risk Management and Audit for comments. Indicate the Level of Assurance given at the audit and whether it contains any outstanding significant recommendations that need to be reported to the Audit Panel or Greater Manchester Pension Fund's Local Board. If no response is received within two weeks send a reminder email.		
4.12	Once review points have been cleared issue PAR (in PDF Format) to all recipients of the Final Report.		
4.13	Update Galileo accordingly		
4.14	Update the PAR Spreadsheet accordingly.		
4.15	Save a copy of the finalised PAR in Galileo.		
4.16	If a follow up PAR is needed, schedule in calendar, update Galileo and the PAR Spreadsheet accordingly.		
4.17	Scan the completed QCC into Galileo		
4.18	When the follow up PAR is due, follow steps 4.1 – 4.17 if applicable.		

Please Note

The corporate standard for report writing is as follows:-

Arial 11 and Justified

2cm Margins

Date Format - xx Month 2015

Audit specific standards:-

Do not use '&'

Do not use don't, haven't etc.

CUSTOMER SATISFACTION QUESTIONNAIRE

To:
Audit
Title:
Auditor:

Date:
Project
Ref:

In accordance with the concept of Continual Improvement, the Internal Audit Section is continually monitoring and striving to improve its methods of operation, with the aim of giving you a better service.

Part of this process involves obtaining your opinion on individual audits, the process adopted and the conduct of audit staff.

Your comments/feedback is important to us, not only will it be used to improve the audit process but also to identify training needs for individual auditors.

	Excellent	Good	Fair	Weak	Unsatisfactory
AUDIT PLANNING					
Consultation on audit coverage, process and timing					
AUDIT PROCESS					
Were interruptions to your operations kept to a minimum?					
How well did we achieve the scope and objectives?					
Did the audit cover the relevant business risks?					
QUALITY OF AUDIT REPORT					
Clarity of report					
How well did we communicate the findings of the audit prior to issuing the draft report?					
Accuracy of audit findings					
Value/practicality of audit recommendations					
TIMING					
Duration of the audit					
Timeliness of the draft audit report					
AUDITOR					
Communication with yourself and auditees.					
At the conclusion of the audit how well did the auditor understand the subject?					
Was the auditor responsive to what he/she was told?					
How well were queries that arose during the audit dealt with?					
EQUALITY					
During the audit process have you been treated fairly with regards to ethnicity, gender, disability, age, religion/belief and sexual orientation?					

If Unsatisfactory or Weak is selected please explain why. We cannot improve without knowing the reasons behind these lower scores.

- A. Was there anything about the audit that you especially liked/disliked?
- B. Do you have any comments about the format of the audit report?
- C. Was the audit useful?
- D. Was the audit relevant?
- E. Have you any suggestions as to how we can improve?

Signed

Date

Thank you for taking the time to complete this questionnaire.
Please return it to Wendy Poole, Audit Manager in Room 2.33a or by email
(wendy.poole@tameside.gov.uk)

INTERNAL AUDIT – PERFORMANCE TARGETS

CATEGORY	DESCRIPTION	NARRATIVE	HOW IT'S MEASURED	TARGET
COMPLIANCE	Public Sector Internal Audit Standards Compliance	Level of compliance with requirements of Public Sector Internal Audit Standards / Local Government Application Note	Annual Self-Assessment / External Assessment (5 yearly)	100%
OUTPUTS	Audit coverage	% of Plan Complete	Audit time recording / workflow management system	90%
OUTPUTS	Audit Impact	% Recommendations Implemented	Audit time recording / workflow management system	90%
QUALITY	Customer Satisfaction	90% of customers "satisfied ≥ 65%"	Customer Satisfaction Questionnaire	100%
OUTPUTS	Fraud Cases	No. of Irregularities Reported/Investigated	Audit time recording / workflow management system	Downward Trend

Tameside Metropolitan Borough Council Internal Audit Service – PSIAS Action Plan

The following points for action to develop the Audit Function arising from the peer review are detailed below:

PSIAS Ref	Ref No.	Points for Consideration	Responsible	Action
1110	1	Consideration should be given to obtaining formal feedback from the Chief Executive and Chair of Audit Committee for the annual appraisal of the Head of Risk Management and Audit.	Director of Finance	The Annual Development Review for the Head of Risk Management and Audit will take on board the recommendation made.
1130	2	Consider allocating the formal SIRO designation to a chief officer, even if the internal audit team continues to support the SIRO function.	Director of Finance/Director of Governance and Resources	The roles relating to Information Governance are being discussed at a meeting on 9 May 2018.
2010	3	Consideration should be given to demonstrating how the audit plan and priorities align to the corporate risk register, assurance framework, link to the Council's objectives and priorities and the prioritisation of audit assignments.	Wendy Poole Head of Risk Management and Audit Services	The Audit Plan for 2018/19 will be presented taking on board this recommendation.
2010	4	The audit plan could be more specific to outline what an optimum level of staff would be able to deliver. This would enable the Audit Panel and Senior Management Team to make an informed assessment of the adequacy of staffing levels.	Wendy Poole Head of Risk Management and Audit Services	The planning process for 2018/19 and future years will incorporate the recommendation made.
1300	5	The Quality Assurance and Improvement Programme (QAIP) should include an action plan identifying steps which will be taken to continually improve the service and enable Audit Panel to monitor progress. The Quality Assurance and Improvement Programme should also be referenced in the Annual Report.	Wendy Poole Head of Risk Management and Audit Services	The Quality Assurance and Improvement Programme (QAIP) for 2018/19 will take on board the recommendation and detail the improvements included in this report as a minimum.

APPENDIX D

During the review the following additional points for consideration were identified. Whilst these specific points are out of scope of the PSIA Standards / LGAN requirements, they are nonetheless contributory to the overall effectiveness and efficiency of the Internal Audit Service and are presented for information and consideration only:

Rec No.	Points for Consideration	Responsible	Action
1	The Audit Plan and Progress reports to Audit Panel are described as reports of the AD Finance/Director of Finance with the Head of Risk Management and Audit also listed as a reporting officer. To ensure that audit retains its organisational independence we recommend that the reports go in the name of the Head of Risk Management and Audit.	Wendy Poole Head of Risk management and Audit Services	This will be discussed with the Director of Finance and Director of Governance and Pensions, as normal practice at the Council is for the Director to be listed then the reporting officer.
2	Consideration should be given to identifying the skills needs by the audit team to assist the Council with its current transformation programme and provide training and development opportunities to address any skills shortage.	Wendy Poole Head of Risk management and Audit Services	This will be discussed with the Director of Finance to ensure the appropriate skills are identified and training and development opportunities to address any skills shortage delivered.
3	Clearer guidance on the extent of post audit review work should be documented in line with the number and priority of recommendations. In addition, improved transparency could be achieved by including post audit reviews in the periodic progress reports to Audit Panel. Consideration should also be given to the process for agreeing extensions to target implementation dates and post audit review timings.	Wendy Poole Head of Risk management and Audit Services	Further enhancements to the progress reports to the Audit Panel were introduced during 2017/18 and the recommendation will be considered for the reporting process for 2018/19.

This page is intentionally left blank

Report To:	AUDIT PANEL
Date:	29 May 2018
Cabinet Deputy/Reporting Officer:	Wendy Poole - Head of Risk Management and Audit Services
Subject:	INFORMATION GOVERNANCE
Report Summary:	To provide an update on the requirements of the General Data Protection Regulations (GDPR) and the new Data Protection Act.
Recommendations:	<ol style="list-style-type: none">1. Members note the report.2. Members approve the Information Governance Framework documents attached at Appendices 1 – 12.
Links to Community Strategy:	Strong information governance supports the individual operations, which deliver the objectives of the Council.
Policy Implications:	Data Protection legislation is changing from May 2018. The Data Protection Act 1998 will be replaced by the General Data Protection Regulations which become effect from 25 May 2018 and a new Data Protection Act. It is therefore critical that policies and procedures are updated to ensure compliance with the new regulations/act.
Financial Implications: (Authorised by the Section 151 Officer)	Non-compliance with the Data Protection Act 2018 or the General Data Protection Regulations can result in the Information Commissioner's Office imposing financial penalties up to maximum of €20 million or 4% of annual turnover (depending on which is larger) for the most serious breaches.
Legal Implications: (Authorised by the Borough Solicitor)	Non-compliance with the General Data Protection Regulations and the new Data Protection Act could expose the Council to an enforcement notice and/or a financial penalty from the Information Commissioners Office.
Risk Management:	Information is a valuable asset to the Council and personal information needs to be protected as privacy failures could be very damaging to the Council in terms of reputational damage and they could have significant financial implications. The necessity to update and refresh our Information Governance Framework and commit the necessary resources within service areas to support the corporate Risk and Insurance Team will be critical if we are to comply with the new requirements of the GDPR and Data Protection Act.

Access to Information:

Background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by contacting:



Telephone: 0161 342 3846



e-mail: wendy.poole@tameside.gov.uk

1. INTRODUCTION

- 1.1 Significant changes are happening in relation to Data Protection legislation in May 2018.
- 1.2 The General Data Protection Regulations (GDPR) come into operation from 25 May 2018 and will effectively replace the current EU derived rules enshrined in the Data Protection Act 1998.
- 1.3 The Data Protection Bill which is currently progressing through the House of Lords contains a number of inter-related objectives and it is envisaged that it will be enacted in May 2018.
- 1.4 It is important to note that GDPR is an evolution in data protection and not a revolution. It demands more on organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. It builds on the foundations already in place for the last 20 years.
- 1.5 Many of the fundamentals remain the same and have been known about for a long time; fairness, transparency, accuracy, security, minimisation and respect for the right of the individual. The General Data Protection Regulations strengthens the controls that organisations (data controllers) are required to have in place over the processing of personal data.
- 1.6 The Information Commissioners Office has produced a guidance document entitled “12 Steps to Take Now” which can be found [here](#), which explains where there is continuity, what’s new and how to plan. This together with the regulations has been used to inform the work plan for the Council which is monitored by the Information Governance Group. As we have an established Information Governance Framework in place, we are developing systems and processes already in place.

2 PURPOSE OF THE REPORT

- 2.1 To provide the Audit Panel with an overview of the work that is ongoing to ensure that the Council has a plan of action in place to move towards full compliance with both the General Data Protection Regulations and the new Data Protection Act 2018.
- 2.2 Whilst 25 May 2018 is quoted as being the date for the General Data Protection Regulations to become effective, the Information Commissioner has clearly stated that 25 May is the beginning of a journey and not the end.
- 2.3 Work has concentrated on the following areas:-
 - Creating information asset registers for all service areas, by facilitating workshops with managers to collate data in a template approved by the AGMA Information Governance Group;
 - Using those registers, to create privacy notices for publication on the public website;
 - Producing a Record of Processing Activities (ROPA) which will need to be published on our website and this will be based on the information asset registers from service areas;
 - Reviewing the Information Governance Framework documents in line with the new requirements;
 - Identifying the best training and communications methods to ensure messages and training reach all staff in the most useable and appropriate way;
 - Producing a Contract Variation letter to be sent to all contractors, suppliers and processors; and
 - The introduction of an Information Governance Newsletter.

3 KEY CHANGES

- 3.1 Down from 8 principles to 6. These are:
- Personal data (anything information that can identify a living individual) must be processed fairly, lawfully, and in a transparent manner;
 - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible;
 - Adequate, relevant and limited to what is necessary;
 - Accurate and where necessary kept up to date;
 - Kept in a form that permits identification of the data subject for no longer than is necessary; and
 - Processed in a manner that ensures appropriate security.
- 3.2 Breaches of personal data that result in a risk to the rights and freedoms of individuals must generally be reported to the ICO within **72 hours**.
- 3.3 Under GPDR, fines can be issued for security breaches and where an organisation cannot demonstrate compliance with any of the Principles. Fines increase up to €20million or 4% of annual turnover (depending on which is larger).
- 3.4 The council must be able to demonstrate that we are compliant with the GDPR, i.e. having appropriate policies and procedures in place for the governance of all personal data processed. This includes keeping a record of:
- what types of information we process;
 - why we process the information;
 - who the information is about;
 - who we share the information with;
 - a general description of our security measures;
 - our retention policy and schedule; and
 - any transfers to third countries outside of the EU.
- 3.5 Sensitive personal data becomes 'special categories' of data.
- 3.6 Consent is a much higher standard. It must be opt-in and clear, explicit and freely given and demonstrable, preferably time limited, and given to the data subject in an age appropriate, plain language format. The data subject must also be informed that they are able to withdraw their consent at any time as easily as it is given.
- 3.7 A Data Protection Officer (DPO) must be appointed.
- 3.8 Subject Access Rights (SARs) are still the cornerstone of the GDPR. However, individuals also have new rights under the GDPR, these new rights include:
- The right to erasure/to be forgotten;
 - The right to object;
 - The right to data portability;
 - The right to rectification;
 - The right to restrict processing;
 - Subject Access Request response time is now 1 month (previously 40 days), this can be extended by a further 2 months if the request is highly complex or large in volume; and
 - The £10 fee is removed.

4 INFORMATION GOVERNANCE FRAMEWORK

4.1 The Information Governance Framework was introduced in 2013 and has been updated since then as new guidance and advice has been received and published by the Information Commissioners Office. The current framework is shown in the diagram below.

4.2 Diagram 1 – Information Governance Framework



4.3 The documents detailed in the table 1 below have been refreshed and updated in light of the General Data Protection Regulations (GDPR).

Table 1 – Information Governance Framework Review

Document Title	Last Updated	GDPR ready? (Y/N)	Appendix No.	Comments
Information Governance Policy	Nov 2016	N	1	The overarching documents have been refreshed and updated to reflect changes made in the supporting documents and to reflect changes to legislation.
Information Governance Conduct Policy	Nov 2016	N	2	
ICT Security Policy	Nov 2013	Y	3	Refreshed and updated to reflect changes to legislation.

Document Title	Last Updated	GDPR ready? (Y/N)	Appendix No.	Comments
Email, Communications and Internet Acceptable Use	Nov 2013	Y	4	Refreshed and updated to reflect changes to legislation.
Social Media Responsible Conduct	Nov 2013	Y	5	This was approved by the Standards Committee in October 2017 and slightly amended now to remove reference to the Data Protection Policy and replace with the Information Governance Framework.
Removable Media Protocol	Nov 2013	Y	6	Refreshed and updated to reflect changes to legislation and definitions.
Mobile and Remote Working Protocol	Nov 2013	Y	7	Refreshed and updated to reflect changes to legislation and definitions.
Access and Security Protocol	Nov 2013	N	8	Refreshed and updated to reflect changes to legislation.
Information Security Incident Reporting Procedure	Nov 2016)	N	9	This document has been refreshed and reviewed to reflect the new requirement to notify the ICO with 72 hours of a notifiable breach.
Secure/Clear Desk Procedure	Nov 2013	Y	10	Refreshed and updated to reflect changes to legislation
Golden Rules	Nov 2013	Y	11	Refreshed and updated to reflect changes made to other documents.
Subject Access Request Guidance	Nov 2016	N	12	The guidance has been updated to reflect that the timescales for responding has reduced from 40 days to 1 month. The fee of £10 has been removed. Extensions will only be granted in exceptional circumstances and the age of consent has been lowered to 13. Information requested needs to be manageable/useable and easy to understand.

- 4.4 The documents detailed in the table 2 below have not been refreshed and updated yet as more work needs to be undertaken in light of the Information Asset audits undertaken.

Table 2 – Information Governance Framework Documents to be reviewed

Document Title	Last Updated	Comments
Retention and Disposal Schedule	Nov 2013	This will be reviewed once the information audits have been completed so that the existing schedule can tailored to the Council.
Managers Checklist	Nov 2013	This will need to be reviewed to reflect changes made to all other documents.
Information Sharing	Nov 2013	Use of consent and privacy notices need to be reviewed, together with individual's rights.

Document Title	Last Updated	Comments
Protocol		Processors will have the same responsibilities as owners.
Data Protection Impact Assessments	New Requirement	The document produced by the Information Commissioner's Office is being reviewed.

5 TRAINING AND AWARENESS

- 5.1 Discussions with People and Workforce Development have commenced to ensure that training and awareness is targeted at the right people in a format that meets their needs. A new Mandatory E-Tutorial - General Data Protection Regulations has been rolled out for completion by the end of June.
- 5.2 Consideration is also being given to delivering some Manager Briefings about the key changes in relation to Subject Access Requests, Reporting Information Incidents and dealing with the new rights for Individuals.
- 5.3 Articles have been published in Live Wire and in the Chief Executive's Brief.

6 RECOMMENDATIONS

- 6.1 Members note the report.
- 6.2 Members approve the Information Governance Framework documents attached at **Appendices 1 – 12.**

This page is intentionally left blank

Information Governance Policy

May 2018

1. INTRODUCTION

- 1.1 Information is a valuable asset that the Council has a duty and responsibility to protect. This responsibility is placed on the Council by the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR) monitored and regulated by the Information Commissioner's Office and the Local Public Services Data Handling Guidelines.
- 1.2 The Information Commissioner's Office now has powers to enable them to impose monetary penalty notices on organisations for up to €20,000,000 or 4% of annual turnover (depending on which is larger) for breaches of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.
- 1.3 The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines Version 4 produced in February 2017 by the Public Services Network in partnership with the Local Chief Information Officer Council, Society of Information Technology Management (Socitm), the Cabinet Office and the National Local Authority Warning, Advice and Reporting Point (NLAARP). The Council therefore has an obligation to comply with these guidelines, to ensure good practice is being followed.
- 1.4 To ensure that information assets and information systems are used and managed effectively, efficiently and ethically, the Council has produced an Information Charter (see Appendix 1), this will work alongside the Information Governance Framework, to ensure everyone is aware of their obligations.

2. PURPOSE OF POLICY STATEMENT

- 2.1 The purpose and objective of this Information Governance Policy is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.
- 2.2 The Council is committed to protecting information through preserving;

Confidentiality: Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

Integrity: Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability: Being accessible and usable on demand by an authorised individual, entity or process.

3. INFORMATION GOVERNANCE FRAMEWORK

- 3.1 This Information Governance Policy is the over-arching document of the Council's Information Governance Framework, (see figure 1 below). The Information Governance Framework comprises of the Information Governance Policy and specific supporting procedures, standards and guidelines as follows:-

- Information Governance Policy and Information Governance Conduct Policy;
- ICT Security Policy;
- Email, Communications and Internet Acceptable Use Policy;

- Social Media Responsible Conduct Policy;
- Data Protection Impact Assessment;
- Removable Media Protocol;
- Mobile and Remote Working Protocol;
- Retention and Disposal ;
- Access and Security Protocol;
- Incident Reporting Procedure;
- Secure/Clear Desk Procedure;
- Subject Access Request Guidance
- Information Asset Registers
- Golden Rules
- Information Governance Managers Checklist
- Information Sharing Protocol

3.2 Figure 1 – Information Governance Framework



4. SCOPE

- 4.1 The Information Governance Policy, along with the Conduct Policy and all supporting documents, apply to all employees, Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.
- 4.2 This Information Governance Policy applies to information in all forms including, but not limited to:-
- Hard copy or documents printed or written on paper;
 - Information or data stored electronically, including scanned images;
 - Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
 - Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
 - Information stored on portable computing devices including mobile telephones, PDA's and laptops;
 - Speech, voice recordings and verbal communications, including voicemail; and
 - Published web content, for example intranet and internet.

5. INFORMATION GOVERNANCE

- 5.1 Information Governance is the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information Governance includes physical, personnel and information security and is an essential enabler towards making the Council work efficiently. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.
- 5.2 The Council is aware that risks can never be eliminated fully and it has in place a strategy that provides a structured, systematic and focused approach to managing risk. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if the Council is to achieve its objectives. The Council seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', the Council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.
- 5.3 Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Governance lifecycle and will apply across the Council and in its dealings with all partners and third parties.

6. RESPONSIBILITY FOR INFORMATION GOVERNANCE

- 6.1 Senior Management (Directors, Assistant Directors and Service Unit Managers) has the responsibility and accountability for managing the risks within their own work areas. Employees have a duty to work safely, avoid unnecessary waste of resources and contribute to Governance initiatives in their own area of activities. The cooperation and commitment of all employees is required to ensure that Council resources are not squandered as a result of uncontrolled risks.

6.2 The Local Public Services Data Handling Guidelines 2017 and EU General Data Protection Regulations (GDPR) specify roles organisations must appoint to in relation to Information Governance as follows:-

- Data Protection Officer
- Accounting Officer
- Senior Information Risk Owner
- Information Asset Owners

6.3 These specific roles together with the Information Governance Group and Information Champions will work together with senior management to ensure compliance with best practice with the over-riding objective to keep the Council's information safe.

6.4 Table 1 below details the roles and responsibilities allocated to key staff.

Data Protection Officer	The Data Protection Officer has the formal responsibility for regulating and approving the application of information legislation for the organisation. (To be determined)
Accounting Officer	The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. (Assistant Executive Director of Finance)
SIRO	The Senior Information Risk Owner is familiar with and takes ownership of the organisation's information governance policy and strategy. (Head of Risk Management and Audit Services)
IAO	Information Asset Owners are Directors/ADs involved in running the relevant Directorate. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
SIAO	Supporting Information Asset Owners are at Service Unit Level and may have more familiarity with the information assets of that particular area. They are required to feedback to IAO's on what information their service area holds and how it is being managed.
System Owners	System Owners are responsible for Information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate and up to date.
Information Champions	Information Champions are senior managers representing services from across each directorate and act as the liaison between the Information Governance Group and staff to ensure the framework, communications and training are effective and reach all staff

This page is intentionally left blank

Information Governance Conduct Policy

May 2018

1. Introduction

- 1.1 Tameside Metropolitan Borough Council (the Council) has a responsibility under the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) to ensure that the personal information it holds and uses is properly protected. To this effect an Information Governance Framework, which is detailed in Appendix 1, has been created to support employees in complying with this responsibility. This conduct policy forms part of the Framework and outlines the expected behaviour of employees regarding information governance. It also indicates the policies, protocols and procedures the Council has put in place to keep its personal information safe.
- 1.2 The Information Governance Conduct Policy applies to all employees, including temporary contract staff and volunteers. It relates to information held both in computerised/electronic systems and paper based records. This includes both work related and personal online activity.
- 1.3 The Information Governance Conduct Policy sits at the heart of the Information Governance Framework providing information and direction for employees on what is deemed to be acceptable behavior not only when dealing with personal information, but also when generally using systems, electronic communication, the internet or social media. It is not intended to restrict service delivery but to raise awareness of the issues and concerns relating to the variety of information risks faced by the Council.
- 1.4 The Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) are the key pieces of legislation covering personal information and the Information Commissioner's Office (ICO) is the regulator and has a range of enforcement actions including the power to fine organisations up to €20,000,000 or 4% of annual turnover (depending on which is larger) for non-compliance.
- 1.5 The Local Public Services Data Handling Guidelines outline best practice for protecting information together with resources provided by the Records Management Society, National Archives, Society of Information Technology Management (SOCITM), Local Authority Information Governance Groups and the Information Commissioners Office (ICO).

2. Procedures

- 2.1 The Council has a number of policies, protocols, procedures and guidance documents that form the Information Governance Framework; these will support and provide clarification on information governance.
- 2.2 Appendix 1 provides a list of each element of the Information Governance Framework with a brief explanation of the content and the key conduct issues from each of the supporting policies, protocols and procedures.
- 2.3 These policies, protocols, procedures and guidance documents, which may be amended from time to time, are available on the Council's Intranet (Staff Portal) or on request from Risk Management and Audit Services (Insurance).
- 2.4 The table shown in Appendix 2 identifies the mandatory minimum documents for employees to read relevant to their role. It is the responsibility of Managers to ensure the appropriate documents have been read and to provide clarification for employees of the relevant role if there is any doubt.

3. Roles and Responsibilities

- 3.1 Employees are accountable and owe a duty of care to the Council, service users and the residents of Tameside, who they act on behalf of and whose information they handle. It is the responsibility of all employees to ensure their use of the Council's information does not infringe any of the Council's policies and procedures. Or, in turn breach the requirements of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR), the Freedom of Information Act 2004 and the Environmental Information Regulations 2004 or any other applicable legislation.
- 3.2 Employees have a responsibility to comply with the Information Governance Framework, when not only handling personal information but also when generally using the internet, any electronic communication or social media. The policies and procedures detailed in Appendix 1 will assist with this compliance.
- 3.3 Managers are responsible for ensuring that employees have appropriate time and support to read the relevant documents and undertake any necessary training. They are also responsible for identifying the relevant policies and procedures for employees to read using the matrix provided. This should be communicated to all employees as part of the induction process, and thereafter as part of team briefings and employee updates. If any assistance is required Managers should contact the Risk Management and Audit Services (Insurance) for advice.
- 3.4 It is the responsibility of Managers to exercise an appropriate supporting and enforcing role for the identified requirements of the Information Governance Framework to minimise the risk of information loss and breaches of legislation.
- 3.5 The public is entitled to expect the highest standards of conduct from employees, when handling personal information. The employees role is to serve the Council in providing, implementing its policies and delivering services to the local community. In performing these duties employees must ensure that they understand the requirements placed on them by the Information Governance Framework.
- 3.6 There is an expectation that all communication from staff, whether handwritten, electronic or verbal, is done so with a high level of professionalism. All communications should meet the 'Chief Executive Test' namely would the Chief Executive say or write this behalf of the Council or more importantly would this communication give the Chief Executive cause for concern if he saw it? All communication, whether written or verbal should be courteous and in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour should be avoided, as it can be misinterpreted. The sending, or forwarding on, of jokes by e-mail (or as an attachment) is strictly prohibited. Any written information can be requested under Subject Access or Freedom of Information, so staff need to think what the impact would be on an individual if they read that information or it was disclosed to a third party.

4. Contraventions of the Policy

- 4.1 Employees need to be aware that this policy and the documents that make up the Information Governance Framework are in place to protect the information held by the Council and to provide assurance to partners, key stakeholders and the residents of Tameside. Failure to adhere to these framework policies, protocols, procedures and guidance documents may lead to disciplinary action being taken and for more serious cases, where individuals have not followed guidance and policies, legal action. In addition it should be noted that an individual fine can be imposed by the Information Commissioner's Office (ICO) in the event that an employee has purposefully used information for an individual's own financial or personal benefit or acted in a highly negligent manner.

INFORMATION GOVERNANCE FRAMEWORK

Information Governance Policy

The Information Governance Policy and Information Governance Conduct Policy are central to the Information Governance Framework and **must** be read by all employees. Further guidance on the information contained within these documents can be found in the supporting framework documents and an Information Governance Framework Mandatory Documents Matrix can be found at Appendix 2 to assist managers and employees in assessing what documents are relevant to their role. To view the Information Governance Policy, [click here](#).

a) ICT Security Policy

This document sets out the responsibilities for using and securing the Council's hardware, software and networks. It details the Council's rights and obligations, and outlines the consequences of using Council Technology in a harassing or abusive manner and the disciplinary implications of not complying with the policy.

Key Conduct Issues

- Protect, at all times, passwords which enable access to data and the Council's network, business systems, email and internet. For further guidance refer to the ICT Freshdesk Service;
- Never use another person's ICT equipment or device without their permission and with anything other than your own credentials;
- Never use, or install, any software on the Council's systems unless it has been purchased, issued or approved by ICT Services; and
- Always save work related information on the Council's network drives and not on local hard drives/desktop. The secure network is backed up and remains available even if your computer fails.

For further guidance [click here](#)

b) Email, Communications and Internet Acceptable Use Policy

This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and Internet facilities, including business and personal use of email (including the personal use of Council and non-Council/personal email accounts). Work related and personal use of the internet (including websites accessed and transactions permitted for work or non-work purposes). It also explains what will happen if Council systems are used for harassment or abuse and the disciplinary implications of not complying with the policy.

Key Conduct Issues

- Never open an email from sources you do not know or trust, and always report unusual emails, suspicious attachments and links, especially in unsolicited emails;
- Never use non-Tameside email accounts to send or receive protected information;
- Use of your @tameside.gov.uk email address is for official Council business, although it can be used for personal business in your own time, this should be kept to a minimum;
- Never send protected information by external email **unless**;
 - You have a GCSX account and are sending it securely to **another GCSX account** (or other secure government networks) or;
 - You are sending it using Egress Switch or;
 - You are sending it in an attachment, using a strong password and encryption software.
- Use of the Council's email and internet systems are monitored and activity is logged.

For further guidance [click here](#)

c) **Social Media Responsible Conduct Policy**

This policy applies to all employees whilst participating in any on-line social media activity, whether privately or as part of your role with the Council. It sets out the standards of behaviour the Council expects of all its employees, when using social media services. The disciplinary implications of inappropriate posting on social media websites are explained. It also advises on using social media safely, legally and appropriately and points out that employees are personally liable for what they publish online.

Key Conduct Issues

- Frequent or excessive non-work related use of social media during the working day is not permitted and may result in the withdrawal of some or all access privileges;
- Employees must NOT conduct themselves in a way that is detrimental to the Council and should NOT act in a way which could damage the reputation of the council or the public's trust and confidence in an employee's fitness to undertake their role;
- Never use the Internet in any way to send or post abusive, offensive, hateful derogatory or defamatory messages or comment, especially those which concern members of the public, councillors, employees or the Council; and
- Never post information that could constitute a breach of copyright or data protection legislation.

For further guidance [click here](#)

d) **Removable Media Protocol**

This protocol aims to ensure that the use of removable media is securely controlled. All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them. Service areas are responsible for implementing this procedure and must monitor the use of removable media. The protocol explains the types of removable media that can be used and the security necessary for use. There is also an explanation of how to dispose of removable media securely. Loss of any unencrypted removable media could result in a potential breach of Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) and subsequent disciplinary action for the employees involved.

Key Conduct Issues

- Only encrypted USB memory sticks purchased through ICT Services may be used in the Council, purchasing must be done through the approved ordering system;
- Information can only be moved from the Council's systems to an encrypted USB stick
- Information held on removable media should be a short term measure;
- Removable media should be kept secure at all times;
- Removable media should be disposed of securely to minimise the risk of accidental disclosure of sensitive information; and
- All removable media connected to the Council's systems is monitored.

For further guidance [click here](#)

e) **Mobile and Remote Working Protocol**

This protocol applies to any access or use outside Council controlled premises of any ICT Council equipment including mobile telephones, portable devices and static IT equipment. All employees are responsible for the safety and security of portable devices and the information on them, issued to or used by them. Explanations of what physical security is required on the devices and how to use them in line with Council policies and procedures are provided.

Key Conduct Issues

- Always ask yourself '*do you really need to take that information out of the office*' and only take the minimum;

- Do not let unauthorised people, including family members, use or view Council resources and avoid ‘*shoulder surfers*’ in public places viewing your screen or listening to business conversations; and
- Make sure your laptop/device is suitably encrypted and if you have encrypted equipment and protected information in physical files overnight in your home, reduce the risk by ensuring that they are placed out of sight.

For further guidance [click here](#)

f) Retention and Disposal Schedule

The schedule outlines the timescales involved for the retention and disposal of information held by the Council. The Retention and Disposal Guidelines will ensure that the information the Council holds is retained for only as long as it is needed to enable it to operate effectively. They also cover the correct disposal methods to be used. Working within the schedule will ensure the Council complies with legislation and the requirements of regulators.

Key Conduct Issues

- Laptops which are no longer required must be returned to ICT enabling the hard drive to be permanently erased;
- Confidential paper waste must be kept separate from ordinary paper waste and protected from accidental loss, damaged or unauthorised access; and
- Information must never be retained for longer than necessary ‘*just in case*’.

For further guidance [click here](#)

g) Access and Security Protocol

This procedure indicates the steps required to ensure that access to Council information, information systems or ICT equipment is controlled. Access needs to be restricted to that needed to perform a role and employees must understand their responsibilities for ensuring the security and confidentiality of information they use. Managers must ensure that access is removed as soon as it is no longer required. It also includes the Leavers and Movers Checklist. As information is held in both paper and electronic format this procedure relates to both physical and technological access.

Key Conduct Issues,

- Access will only be granted to systems and information where it is part of your role and you have a legitimate business need to know;
- Where you need protected information ‘owned’ by another business area to do your job, make sure that authorisation is obtained and that you only ask for the minimum necessary for the required purpose.

For further guidance [click here](#)

h) Incident Reporting Procedure

This procedure must be applied immediately as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident (ISI). All incidents, irrespective of scale, must be reported immediately to ensure that a thorough understanding of what has occurred is recorded, to improve information handling procedures, the incident response process and any subsequent action that may be required. Where a breach is established to have occurred we are required to report to the Information Commissioners Office within 72 hours. Failure to report an incident may result in **disciplinary action** being taken.

Key Conduct Issues

- You must always report actual, potential or suspected security violations, problems or vulnerabilities to the Risk and Insurance Manager, ICT Security Officer or Legal Services

For further guidance [click here](#)

i) **Secure/Clear Desk Procedure**

This procedure reduces the threat of a security breach as information should be kept out of sight. This procedure applies to all information of a personal, confidential or sensitive nature. It also covers any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point). If non-compliance of this policy results in a breach of the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR) subsequent disciplinary action for the employee could arise.

Key Conduct Issues

- Never leave protected information or other valuable assets out on your desk when you are not around;
- Lock your work station when you are away from your desk using *Ctrl + Alt + Delete*, log off at the end of the day and switch off your screen; and
- Remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else.

For further guidance [click here](#)

j) **Subject Access Request (SAR) Guidance**

This guidance has been drawn up to assist employees in understanding how to recognise and respond to a SAR in compliance with the Council's obligations under the DPA. It explains the right of access to personal data and the procedures that must be followed.

Key Issues

- Individual's data rights are set out in the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR).
- The right of subject access allows a living individual ("the data subject") to find out what information ("personal data") is held by an organisation about them;
- All SARs should be responded to promptly, and in most cases the maximum time limit for responding to a SAR is 1 calendar month once the complete request has been received by the Council;
- In some cases exemptions may be applied, which means that certain information may not need to be disclosed to the data subject in response to their SAR;
- Where a requester is not satisfied with the response to their SAR, the Council offers an internal review. In addition to the internal review process, a data subject may also refer their complaint to the ICO, or may take action through the courts to enforce their right of subject access.
- A failure to follow this guidance may result in **disciplinary action**.

For further guidance [click here](#)

k) **The Golden Rules**

These Golden Rules aim to help you safeguard the Council's valuable information assets, systems and equipment. They briefly outline how to use information assets responsibly within the framework of the law and ensure employees understand the corporate policies to comply with. It signposts the mandatory corporate on-line training employees must undertake. All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework. Employees also need to adhere to any localised business specific data handling requirements.

For further guidance [Click here](#)

l) **Information Governance Managers Checklist**

This checklist has been provided for Managers/Supervisors to enable them to identify the areas they should be considering on a regular basis to ensure compliance with the Information Governance Framework. It also details the available resources to assist Managers/Supervisors in complying with the appropriate actions required.

For further guidance [Click here](#)

m) Information Sharing Protocol

This protocol is the overarching document that outlines the responsibilities of employees when sharing information. It applies to all sharing of information, potentially internally and externally to the Council. Information Sharing or Processing Agreements will govern specific exchanges of information and will specify what information is to be shared, how it will be shared and for what purpose the information is required. Failure to comply with this protocol, when sharing information would constitute a breach of the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR) and could result in **disciplinary action**.

Key Conduct Issues

- Before disclosing protected information to an external third party, always ask yourself '*is this request legitimate*' and '*do I need a sharing or processing agreement*';
- Always make sure you have the legal authority to share;
- Check whether the purpose could be satisfied with anonymised or pseudonymised information; and
- Keep a documented audit trail of all disclosures.

For further guidance [click here](#)

n) Data Protection Impact Assessment

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

For further guidance [click here](#)

Information Governance Framework Mandatory Documents Matrix

Framework Document	Managers	Office Based Employees	Office Based with some Home Working	Mobile Working	Care Workers	Manual& Outdoor Workers
Information Governance Policy	✓	✓	✓	✓	✓	✓
Information Governance Conduct Policy	✓	✓	✓	✓	✓	✓
ICT Security	✓	✓	✓	✓	✓	✓
Email, Communications /Internet Acceptable Use	✓	✓	✓	✓	✓	✓
Social Media Policy	✓	✓	✓	✓	✓	✓
Data Privacy Impact Assessments	✓	If Applicable	If Applicable	If Applicable	If Applicable	-
Removable Media	✓	✓	✓	✓	✓	-
Mobile/Remote Working	✓	✓	✓	✓	✓	-
Retention and Disposal	✓	✓	✓	✓	✓	-
Information Access Procedure	✓	-	-	-	-	-
Information Reporting Procedure	✓	✓	✓	✓	✓	✓
Secure/Clear Desk	✓	✓	✓	✓	✓	-
Bring your own Device	✓	✓	✓	✓	-	-
Information Sharing Protocol	✓	If Applicable	If Applicable	If Applicable	If Applicable	-
Golden Rules	✓	✓	✓	✓	✓	-
Managers Checklist	✓	-	-	-	-	-

This page is intentionally left blank

ICT Security Policy

May 2018

1. Introduction

- 1.1 ICT is an increasingly integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council ICT in the course of their duties. This policy is designed to enable the Council to:
- Get the best return possible for the investment it has made in technology;
 - Comply with the law;
 - Minimise legal and other risks associated with the use of technology;
 - Ensure effective running of the Council's business;
 - Minimise the risk of disruption caused by computer viruses and inappropriate use of ICT; and
 - Provide clear information to employees and councillors and increase the ICT skills of our employees and residents.
- 1.2 This policy sets out the Council's policy on using its computers and networks, including all devices such as telephones, mobile phones; faxes; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is for clarity of understanding referred to throughout this policy as the Systems.
- 1.3 This policy applies to all Council employees and Members who use the Systems. It also applies to other people using the Systems such as agency workers and contractors' staff.
- 1.4 Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of your Service Unit Manager or above or the Head of ICT Services.
- 1.5 The Council's Systems are the property of Tameside MBC. In order to protect the Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trades unions.

2. User Responsibility

- 2.1 All users have responsibility for the technology they use. Responsibility extends from the Service Unit Manager who oversees a complete system to individual employees with a PC/Laptop on their desk. Everyone using ICT must observe the following:
- **Equipment Purchase/Disposal** – all Council equipment must be purchased through ICT Services using the Agresso procurement facility. All equipment must be disposed of through ICT services to ensure that legislation is complied with both in respect of the environment and security of information. Changing hard drives; moving ICT equipment or disposing of it without taking appropriate measures to keep information secure is likely to result in confidential information becoming available to persons not entitled to the data and consequentially breaches in statute – requirements to be followed can be found in the [ICT Equipment Disposal Policy](#)
 - **Equipment Maintenance** - if equipment malfunctions you should contact the ICT Freshdesk for advice and assistance. Employees are not permitted to attempt to repair or maintain their ICT equipment, except for day-to-day needs such as replacement ink cartridges in printers etc. Equipment must be kept clean, especially screens and keyboards, and this is the responsibility of the employees using the equipment.
 - **Accidental Damage** - employees are expected to make efforts to avoid circumstances that may result in accidental damage, such as spilt coffee or equipment being dislodged off desks.
 - **Keep Equipment Safe and Secure** - employees should ensure that the equipment provided is kept secure from theft. This particularly applies to portable equipment

such as laptop computers and mobile phones. . If Equipment is lost or damaged as a result of an employee's negligence then disciplinary action may be taken and the Council may take action to recover the loss from the employee concerned. Any queries about this should be referred to Risk Management and Audit Services (Insurance).

- **Equipment Insurance** – Laptops are insured if outside Council premises providing that they are kept secure, out of sight and locked in the boot of a vehicle whilst in transit. However, these portable items are only covered within the UK and must be secured when not in use. Any queries about this should be referred to Risk Management and Audit Services (Insurance).

3. Management of Data, Information and Software

3.1 Employees are expected to manage data in compliance with the law, particularly the law relating to data protection and freedom of information. The Information Governance Framework and supporting policies, protocols, procedures and guidance documents provide additional support, but the main principles are that employees must:

- **Keep data accurate and up to date and retain for no longer than necessary;**
- **Keep Data Secure; and**
- **Keep Data Confidential**– The Council has legal duties under the Data Protection legislation and the Computer Misuse Act to protect the information that it holds. No personal information should be disclosed unless you are sure that you are permitted to do so. When sharing such information with third parties, checks should be made to ensure that third parties are registered as a data controller under the Data Protection Act 1998. Your manager or supervisor will be able to advise you in the first instance. If any employees have any further queries they should seek advice from the Council's statutory Monitoring Officer who is also the Data Protection Officer – Borough Solicitor.

4. Authorised Business Use

- 4.1 You may use the Systems where you have a legitimate business need to do so and the use is appropriate to your role or you are using the Systems for appropriate personal use in accordance with section 9 of this policy.
- 4.2 In order to ensure accountability in the use of the Systems, you must never use any computing device without the permission of the main allocated user.
- 4.3 Communications sent via the Systems represent the Council. Therefore, you must ensure that all messages, communications and information created by you on the Systems are professional in tone and content. The style and language of any messages, communications or information you create should be in accordance with standard business communications and any corporate formatting and style requirements.

5. Unauthorised Use

5.1 You must never use the Council's Systems to:

- Create, review or transmit material that is offensive, untrue, defamatory, malicious, potentially damaging to the Council's reputation or disruptive in nature. In particular you are not permitted to use the Systems to create, review or transmit material containing inappropriate sexual references, discriminatory, harassing or threatening comments, or any other form of communication that would be deemed offensive in

nature and contrary to the Council's employment policies, specifically the Council's Equal Opportunities Policy, Bullying and Harassment Policy and the Information Governance Policy. For the avoidance of doubt this includes but is not limited to material containing nudity, racist remarks, and/or defamatory material;

- Access any part of the ICT facility beyond the facilities available from the main user menus or icons unless you have the Council's permission to do so;
- Use any software that has not been officially purchased, issued or approved;
- Copy any of the software on the Council's Computer Systems without the authorisation of the Council. Software will be audited on a regular basis;
- Alter the configuration of the Council's Systems, hardware or software, without prior authorisation by the Council's ICT Service (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute alteration of configuration of Council Systems;
- Create or circulate chain letters or jokes; nor
- Play computer games.

6. Passwords and Security

- 6.1 You will be issued with passwords for accessing the Council's Systems. You must keep your password confidential and you should not disclose your password to anyone else unless you have been authorised to do so by the Council. You must not write down your passwords or display them where they could be seen by others. You must take care to see that people do not see you entering your password.
- 6.2 It is the Council's policy that passwords should, be changed at regular intervals. During the course of your employment you are likely to be responsible for creating some of your own passwords. When creating a password, you should not select a password that can easily be deduced by others; in particular, you should not use passwords which are easy to guess (e.g. the names of partner children or pets). It is advisable to use a mix of characters, e.g. 3 out of four of: upper or lower case alphabetic characters, numbers and symbols in each password. For further guidance please refer to the ICT Service Portal for Password Guidance, [Click here](#) and type 'password' in the search box.
- 6.3 When you have logged into any computer you should ensure that it is left securely so that no unauthorised person can access it. On Laptops/PCs you can do this by selecting control, alt, delete and using the menu to lock your computer.
- 6.4 Personal or confidential data belonging to or held by or on behalf of the Council or its partners must not be stored on removable media, such as USB memory sticks CDs or external hard drives without the express permission of the Council. Where such information is unavoidably stored on a memory stick, it must be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused. For further information, please refer to the [Removable Media Protocol](#).
- 6.5 When an employee leaves the Council, their access to computer systems and data must be deleted on the employee's last working day. It is the responsibility of the line manager to request access deletion via the ICT Freshdesk. Similarly, Managers must inform ICT Services when any employees change jobs within the Council so that systems can be amended and the user's systems access changed, as appropriate. For more information, see the [Access and Security Protocol and Movers Checklist](#).

7. Approved / Unapproved Equipment and Software

- 7.1 You must not use or install any software on the Systems unless that software has been approved and issued by the Council. For example, you must not install or run software that

you have brought in from home, downloaded from the internet or other ICT Systems. This is to avoid conflicts between software, damage to Systems or breaking copyright law. The ban on installing or downloading software unless specifically authorised by the Council includes a ban on installing or downloading:

- Games
- Freeware and shareware
- Upgrades to existing software
- Demonstration versions of software
- Screensavers

- 7.2 You must not connect any equipment to the Council's Systems unless it belongs to the Council or you have the Council's permission.

8. Unauthorised Access or Modification of Systems

- 8.1 Unless you have been authorised by the Council to do so you must not, nor attempt to, modify the Council's Systems. (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute modification of Council Systems.)
- 8.2 You must not misuse the Council's Systems by accessing information which you are not authorised to view or use, or to attempt to break ('hack') into any computer system, for example by using someone else's password.

9. Personal Use

- 9.1 The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the Council permits you to use the Systems for personal use.
- 9.2 You must not use the Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of Systems to interfere with your day to day duties. Excessive non-job related use of the Systems during contractual hours may be subject to disciplinary action.
- 9.3 You must not use Council software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.
- 9.4 Use of the Systems should at all times be strictly in accordance with the provisions of paragraph 5.1 above. You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls.
- 9.5 You are responsible for any non-business related files which are stored on your computer. If you connect your personal memory stick to any system you must carry out appropriate virus checks first.
- 9.6 When accessing the internet for non-work purposes you may only view web pages and download .pdf files. You may not download other files because they contain a risk of contamination by viruses and that risk is disproportionate to the benefits to the Council in allowing you access to them.

10. The Council's Rights and Obligations

- 10.1 The Council reserves the right to monitor all communications and information created, or transmitted on the Systems in order to protect the Council's legitimate business interests and the Systems. These include, but are not limited to, ensuring compliance with policies, detecting or preventing crime, recording evidence of business transactions and detecting viruses. You should not therefore expect communications conducted on the Council's Systems to be private and confidential.
- 10.2 Any information that the Council collects as a result of monitoring the use of its Systems will be processed in accordance with the Council's Data Protection and Freedom of Information Policies.

11. Viruses

- 11.1 Computer viruses have the potential to cause enormous damage to Systems and the data they hold, and severely affect service delivery as a result. Every effort must be made to avoid introducing viruses into the Council's Systems and equipment, and employees have a clear responsibility in this respect. Employees must ensure that ANY disk or memory stick being brought into the Council is virus checked before loading. If a PC does not have its own virus checking software then the ICT Freshdesk should be contacted
- 11.2 Viruses may be transmitted through E-mails and/or attachments. If anyone has any doubt about an e-mail received, especially from an unknown source, refer it to the ICT Freshdesk. Do not open any suspicious e-mail or attachment. Any employee who intentionally or negligently causes a virus to affect Council Systems is liable to disciplinary action. It is essential that all employees remain vigilant.
- 11.3 To prevent viruses damaging the Systems, all computer Systems must have the appropriate anti-virus software installed and this must be updated regularly. The anti-virus software should never be disabled. All files used on Council computer systems will be scanned automatically but for added security you should take due precautions when using any external device or media such as CDs, USB memory sticks and the like and satisfy yourself that they are virus free. For further information, please refer to the [Removable Media Protocol](#).

12. Use of ICT at home or Out of the Office

- 12.1 The provisions of the Policy apply equally when working on Council data or equipment outside Council premises.
- 12.2 If employees are working from home on a regular/permanent basis then specific arrangements must be agreed with your Service Unit Manager.
- 12.3 Employees must not install Council owned software on their own equipment or connect Council owned equipment to their personal equipment.
- 12.4 The Council cannot be held liable if, for any reason, the use of personally owned equipment for Council business results in that equipment being damaged or adversely affected in any way.
- 12.5 Data must be kept securely. Employees must not use their own equipment to process personal data without the agreement of their Service Unit Manager, who must ensure that proper arrangements for the security of the data are made.

- 12.6 You must not store Council files on your personal equipment. You should use a Council memory stick, which is encrypted, to store such files when working on them at home. Care should be taken to ensure that:-
- a) You do not store files on your computer; and
 - b) When you dispose of any ICT equipment you make sure that no Council documents have accidentally been stored on it and none are stored in any temporary folder – or you remove and destroy the computer's hard drive.
- 12.7 For full details on the use of ICT at home or out of the office, refer to the [Mobile and Remote Working Protocol](#).

13. Ownership Rights

- 13.1 Work related information, communications or data created, received, stored or transmitted by you whilst you are employed by the Council (whether inside or outside of working hours) is and remains the property of the Council.

14. Health and Safety – Display Screen Equipment (DSE) Regulations

- 14.1 All employees have responsibility for Health and Safety in the workplace, and this will be reflected in the manner that ICT is used. Employees and Service Unit Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation. Employees and Service Unit Managers are expected to ensure that the workplace is kept tidy, and that the presence of technology in the office is not a cause for concern.
- 14.2 So far as the Council is concerned, an employee falls within the requirements of the Display Screen Equipment (DSE) regulations if they use equipment for continuous spells of an hour or more (on average) every day. The requirements of the DSE regulations can be found [here](#) and all employees and Managers should comply with them.

15. Back Ups

- 15.1 It is vital that backup procedures are in place to maintain the availability, integrity and confidentiality of data. ICT Services backup the corporate servers on a regular basis.
- 15.2 All employees must be aware that ICT only back up information stored on the network (shared drives). Information stored on local (C:) drives or the desktop is not backed up and would not be able to be recovered if the equipment was lost, corrupted etc. Therefore, information stored on local drives should be kept to a minimum.
- 15.3 Service Unit Managers are responsible for ensuring that appropriate backups are undertaken for any local drives or standalone PCs located in their service area.

16. Harassment and Abuse

- 16.1 The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current '[Bullying and Harassment](#)' policy. Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action

will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to harassment or abuse.

17. Contraventions of the Policy

- 17.1 Local Government employees are expected to give the highest possible standard of service to the public. Employees are expected, through agreed procedures and without fear of recrimination, to bring to the attention of the Council any deficiency in the provision of service. Employees should report to the appropriate manager any impropriety or breach of procedure or misuse of Council property. The Council has a [Whistle Blowing Policy](#) in place to encourage and protect responsible employees to come forward, anonymously if they wish, to report instances of abuse of time, etc.
- 17.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.

18. Disciplinary Implications

- 18.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under Data Protection legislation and the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.
- 18.2 Most use of ICT is by employees and the code has been written with them in mind. However, it applies equally to Councillors using Council owned ICT equipment. Mis-use of Council owned ICT equipment or software may be a breach of the statutory Code of Conduct for Councillors - in which case it may be reported to the Standards Board for England and/or the Council's Standards Committee who may impose a sanction.

Email, Communications and Internet Acceptable Use Policy

May 2018

1 Introduction

- 1.1 ICT is an integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council ICT in the course of their duties. This policy is designed to enable the Council to:
- get the best return possible for the investment it has made in technology;
 - gain maximum benefit from email and the internet;
 - comply with the law;
 - minimise legal and other risks associated with the use of technology;
 - ensure effective running of the Council's business;
 - minimise the risk of disruption caused by computer viruses and inappropriate use of ICT; and
 - Provide clear information to employees and councillors and increase ICT skills of our employees and residents.
- 1.2 This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and internet facilities, including;
- Work related and personal use of email (including personal email accounts);
 - Work related and personal use of the internet; and
 - Work related and personal use of social media (including the posting of information on social media sites whether related or unrelated to any Council business).
- 1.3 This policy applies to Council employees, Members, agency workers, contractors, third parties and all partners who use the technology set out in 1.2.
- 1.4 Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of your Service Unit Manager or above or the AED of Digital Tameside.
- 1.5 The Council's Systems are the property of Tameside MBC. In order to protect the Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trades unions.

2 Personal Use

- 2.1 The Council has devoted time and effort into developing the ICT systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the systems for non-work related purposes, and in recognising this need the Council permits you to use the systems for personal use.
- 2.2 You must not use the systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working. You must not allow personal use of systems to interfere with your day to day duties.
- 2.3 You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls
- 2.4 You must not store personal files on Council systems as there is a cost to the public purse for such storage and backup of the same. You may however use 'Cloud' or on-line storage facilities (using your own personal account). If you connect your personal memory stick to any system you must carry out appropriate virus checks first. If your memory stick is not encrypted you will not be able to save any files to it.

- 2.5 When accessing the internet for non work purposes you may only view web pages and download .pdf files and images. You may not download other files because they contain a risk of contamination by viruses and that risk is disproportionate to the benefits to the Council in allowing you access to them. The Council's filtering system will prevent you from downloading programmes.

3 Email Use

- 3.1 The Council has developed its email system to facilitate effective business communication within the workplace. You are only permitted to use the email system for personal use in accordance with section 2 above – though you should be aware that all emails may be subject to monitoring and the right to send personal emails implies no confidentiality. All emails that you create should adhere to the provisions of this policy, and in particular comply with the requirements set out in this section.
- 3.2 Employees should treat e-mail communications with the same degree of care and professionalism as they would a letter sent out on company-headed notepaper. They should all meet 'the Chief Executive Test' namely would the Chief Executive send this email out on behalf of the Council or more importantly would this e-mail give the Chief Executive cause for concern if he saw it? E-mails should be courteous and written in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour should be avoided, as it can be misinterpreted. The sending, or forwarding on, of jokes by e-mail (or as an attachment) is strictly prohibited.
- 3.3 The sending, or forwarding on, of curt, rude, sexually explicit, racially biased or offensive e-mails (or attachments) is strictly prohibited. Equally, employees are advised not to send e-mails in the heat of the moment. Employees should not send unsolicited, irrelevant, or inappropriate e-mail messages internally or externally, nor should they participate in chain or pyramid letters by e-mail. Furthermore, personal opinions should not be presented as if they were those of the Council.
- 3.4 You should not use the email system in breach of any of the Council's employment policies, particularly the Council's Equal Opportunities Policy, Bullying and Harassment Policy and Data Protection Policy. Employees must not use the e-mail system to send inappropriate messages or images via the email system (whether internally or externally). Inappropriate messages would include those, which are:
- Sexually explicit;
 - Offensive (whether to the recipient or to a third);
 - Potentially damaging to the Council's reputation and/or standards expected by the public;
 - Defamatory;
 - Discriminatory (e.g. racist or sexist); and
 - Constitute harassment (see section 6).
- 3.5 Standard e-mail is not a suitable medium for the communication of confidential, personal, or other sensitive information unless you have been granted permission to do so by the Council; you should not send confidential information by standard email. Confidential information means all information which may be imparted in confidence or be of a confidential nature including but not limited to all information relating to the Council's business or prospective business. It is important to remember that email sent over the internet is not secure. You should not therefore send any confidential information by external email unless it is properly encrypted Email sent by GCSX (where available) is considered to be secure as is the use of Egress Switch.

- 3.6 Email is not a suitable medium for communication on any matter that requires dialogue or discussion and should not be used as a substitute for face-to-face communication.
- 3.7 E-mail is a 'publication' for the purposes of the law. Any e-mail that includes information taken from another source (such as a publication or a website) may also breach copyright, for which the Council may be held responsible. Messages sent via the email system can give rise to legal action against the Council. Claims of defamation, harassment and breach of confidentiality or contract could arise from a misuse of the Systems. Email messages are disclosable in any legal action commenced against the Council relevant to the issues set out in the email. Employees should note that E-mail messages and any attachments can be used as evidence in many circumstances and may have to be disclosed under the Freedom of Information Act. You must use the Council's email disclaimer on emails along with a signature file providing contact details. Anyone found to be sending or forwarding inappropriate messages, or exposing the authority to legal action, may be subject to disciplinary action.
- 3.8 As with other forms of business communications, you should retain copies of the emails you send, where necessary, for an appropriate length of time. Please refer to separate guidance on this matter.
- 3.9 If an email message is sent to you in error, you should contact the sender. If the email message contains confidential information you must not disclose or use that confidential information. If you receive an email of this nature you should contact your immediate line manager.
- 3.10 You should only open emails with attachments from persons or organisations that you are familiar with. If you receive an email with an attachment from an unknown source and you are suspicious as to the nature of the communication you should forward the email to ICT Services to inspect before opening it. You should not open any emails which do not appear to relate to Council business and seem to contain jokes, graphics or images; as such emails regularly contain viruses.
- 3.11 Employees are permitted to send and receive personal email whilst at work (in accordance with section 2 above) but emails must not contain inappropriate content. Employees must not send or receive excessive numbers of personal emails and must not allow their Council email account to be used for commercial (non-Council) purposes. Excessive or inappropriate use of email may lead to disciplinary action and to withdrawal of some or all privilege.

4 Telecommunications

- 4.1 Employees are allowed to use the Council telephone system (and mobile telephones provided by the Council) for personal calls. However, where a cost is incurred employees will reimburse the Council with the cost of the call. Employees will not use telecommunications systems and equipment provided by the Council for any activity that is illegal, for harassment or abuse of others, or for personal gain. Any employee found doing so may be liable for disciplinary action.
- 4.2 Interception and Monitoring: This Policy has been prepared in accordance with Data Protection legislation, the Human Rights Act, and the Regulation of Investigatory Powers Act 2000. Exceptionally, the Council may monitor and/or intercept telecommunications Systems where permitted by the Regulation of Investigatory Powers Act 2000.

5 Internet Use

- 5.1 You may be able to access the internet from the Council's Systems. The internet may be used for legitimate business purposes or for personal use in accordance with section 2. Excessive non-job related use of the internet during the working day may be subject to disciplinary action. Internet access may be withdrawn if it is being abused. Employees should be aware that all visits to websites on the Internet are logged and monitored by software operating on the Council's web server and may be subject to audit and inspection and disclosure under the Freedom of Information Act.
- 5.3 You should try to ensure that you will not be infringing any copyright or related rights, by downloading the information.
- 5.3 You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council's Equal Opportunities Policy and/or the Council's Bullying and Harassment Policy
- 5.4 You should note that, in order to protect its legitimate business interests and its systems, the Council monitors its internet use.
- 5.5 The Council has installed software to try to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and racist sites. The risk of viruses and other malware also means that access to web-based email services is considered inappropriate. However the system relies on a list of banned sites and key word searches and so is not completely comprehensive. Employees are not permitted to access any site with inappropriate content and may be subject to disciplinary action if they do. Exceptionally, employees may need to access this type of site for work related purposes. If this need arises they must seek written authority to do so from the AED Digital Tameside or his Service Unit Managers; the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.
- 5.6 It may, very rarely, happen that despite the protection systems, an employee accidentally visits an inappropriate site. If this happens then they must inform the AED Digital Tameside or his Service Unit Managers and the Head of Risk Management and Audit Services immediately by e-mail to avoid the possibility of being suspected of seeking to access inappropriate web pages.
- 5.7 Employees may use the internet to carry out their own private transactions (e.g. the purchase of books or tickets) in their own time but you may not carry out transactions, which would be viewed as inappropriate under other parts of this Policy. The Council will not accept any responsibility for any loss that you may suffer as a result of personal use of the internet. Employees are reminded that the Council does monitor internet use.

6 Harassment and Abuse

- 6.1 The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current ['Bullying and Harassment'](#) policy. Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to the harassment or abuse.
- 6.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful

purpose.

7 Disciplinary Implications

- 7.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.
- 7.2 Most use of ICT is by employees and the code has been written with them in mind. However, it applies equally to Councillors, contractors, agency staff and other third parties using Council owned ICT. Mis-use of Council owned ICT equipment or software may be a breach of the statutory Code of Conduct for Councillors - in which case it may be reported to the Standards Board for England and/or the Council's Standards Committee who may impose a sanction.

Social Media Use: Responsible Conduct Policy

May 2018

SOCIAL MEDIA USE: RESPONSIBLE CONDUCT POLICY

This policy covers all employees, agency workers and consultants representing the Council.

CONDUCT

As an organisation, we encourage communication among our employees, residents, customers, partners, and others - and Web logs (blogs), social networks, discussion forums, wikis, video, and other social media - such as Twitter - can be a great way to stimulate conversation and discussion. They are also an invaluable tool to share information and consult.

The Internet provides a number of benefits in which Tameside council employees may wish to participate. From rediscovering old school friends on *Facebook* to keeping up with other people's daily lives on *Twitter* or helping to maintain open access online encyclopaedias such as *Wikipedia*. Even if your social media activities take place completely outside of work, as your personal activities should, what you say can have an influence on your ability to conduct your job responsibilities, your work colleagues' abilities to do their jobs, and Tameside's business interests.

Accordingly, where an employee is clearly identifiable as being an employee of the Council and/or discusses their work, they are expected to behave appropriately when on the Internet, and in ways that are consistent with the Council's values and policies. This guidance note sets out the principles which Council employees are expected to follow when using the Internet and gives interpretations for current forms of interactivity. It applies to blogs, to microblogs like *Twitter* and to other personal web space. The Internet is a fast moving technology and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The intention of this guidance is not to stop Council employees from conducting legitimate activities on the Internet, but serves to flag-up those areas in which conflicts can arise.

Tameside Council's reputation for impartiality, objectivity and fairness is crucial. The public must be able to trust the integrity of Tameside councillors, employees and its services. Our residents and partners audiences need to be confident that the outside/private activities of our employees do not undermine the Council's reputation and that its actions are not perceived to be influenced by any commercial or personal interests.

To this end employees/agency workers and consultants:

- Should NOT engage in activities on the Internet which might bring the Council into disrepute;
- Should NOT conduct themselves in a way that is detrimental to the Council;
- Should NOT use the Internet in any way to send or post abusive, offensive, hateful or defamatory messages, especially those which concern members of the public, councillors, customers/service users, employees, agency staff, consultants or the Council;
- Should Not 'like' a comment of this nature;
- Should NOT post derogatory or offensive comments on the Internet;
- Should NOT act in a way which could reputationally damage the council;
- Should NOT act in a way that damages the Council's or the public's trust and confidence in an employee's fitness to undertake their role;
- Should act in a transparent manner when altering online sources of information;
- Should NOT post information that could constitute a breach of copyright or data protection legislation;
- Employees (including agency workers and consultants) should only use their work email addresses for official Council business;

APPENDIX 5

- Should NOT use the Council's ICT Systems for party political purposes or for the promotion of personal financial interests; and
- Should take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees (including agency workers and consultants) and the public.

Individuals in politically restricted posts (usually over salary scale point 44), those that provide regular advice and support to committees and panels or speak with the press and those that work in politically sensitive areas should not be seen to support any political party or cause. Any online activities associated with work for the Council should be discussed and approved in advance by a senior council manager.

All employees (including agency workers and consultants) should be mindful of the information they disclose on social networking sites. Where they associate themselves with the Council (through providing work details or joining a council employee network) they should act in a manner which does not bring the Council into disrepute. Employees (including agency workers and consultants) need to be mindful that even though they do not associate themselves with the Council, others on the social networking site may be able to identify them and make the association.

Employees will be aware that use of the internet at work is provided primarily for business use. However the Council recognises that many employees use the internet for personal purposes and that many employees participate in social networking on websites such as Facebook, Twitter, Myspace, Bebo and Friendster (this list being for illustrative purposes only). Alongside such social networking sites the internet also offers employees the opportunity to access and post on blogs, twitter, wikis and other online forums.

The purpose of this guidance is to outline the responsibilities of employees using social networking websites and other online forums. It forms part of the Council's existing Information Governance Framework and the Councils Employee Code of Conduct.

Personal use of the internet at work

The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the ICT Systems for non-work related purposes, and in recognising this need the Council permits you to use the ICT Systems for responsible personal use.

You must not use the ICT Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of the ICT Systems to interfere with your day- to-day duties or of others.

If you choose to use the Council's ICT Systems to access social networking sites and/or other online forums, blogs etc. you must do so in a responsible and appropriate manner. There is no unconditional right for an Employee to access such sites and the Council reserves the right to restrict access to the internet (or certain websites) for particular employees if there is cause for concern over their use.

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private.

Personal conduct whilst in work or outside the workplace

The Council respects an employee's right to a private life. However, the Council must also ensure that confidentiality and its reputation are protected.

APPENDIX 5

Employees are reminded of the unique way in which information posted on the internet can be quickly disseminated and control over such information can be rapidly lost. As such, employees should think about what information they are posting and how this could reflect on them and the Council especially in light of the difficulty they may encounter in trying to remove such information. Where comments are removed there is no guarantee that removing the source comment removes it from all websites.

Employees (including agency workers and consultants) using social networking websites and/or online forums outside of work are requested to:

- Refrain from commenting on any aspect of the Council's business, on any Council policy issue or issues at work. Adding a disclaimer that the views are your own and not those of the Council, will not protect you from potential disciplinary action should concerns be raised or reported;
- Ensure that they do not conduct themselves in a way that is detrimental to the Council;
- Never send or post abusive, offensive, hateful or defamatory messages about members of the public, councillors, other employees (including agency workers and consultants), customers, service users or the Council; and
- Take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees (including agency workers and consultants), customers, service users and/or members of the public.

Monitoring of online access at work

You should note that, in order to protect its legitimate business interests and its ICT Systems, the Council monitors internet use in accordance with the provisions set down in the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy, and unacceptable levels of use could lead to disciplinary action.

Inappropriate Posting

If an employee is found to have posted inappropriate material in any format on the internet, they are required to assist in any way to ensure such material is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

Disciplinary Implications

If the Council finds that an employees' internet use is not in accordance with the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy or this guidance, access to the internet may be withdrawn.

Employees are reminded they should never send or post inappropriate, abusive or defamatory messages on the internet either whilst in work or outside the workplace. Any messages which are abusive, offensive or defamatory could cause damage to the council's reputation and distress and anxiety to others in the workplace and employees are reminded of their obligations under the Council's Code of Conduct, Equalities Policy and Information Governance Framework.

Employees must be aware that if such matters do come to light, disciplinary action may be taken in line with the Council's Disciplinary Procedure if deemed sufficiently serious, this could result in dismissal.

Security and identity theft

Employees are reminded to be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites and online forums allow people to post detailed personal information

APPENDIX 5

such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

Employees must take care when posting such information, in order that it does not allow a breach of security within the Council, or raise the possibility of the employee's identity being stolen.

In addition, employees should:

- Ensure no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information belonging to the Council, councillors, other employees and/or members of the public; and
- Refrain from recording any confidential information regarding the Council, councillors other employees and/or members of the public on any social networking website.

WHAT IS SOCIAL MEDIA?

Facebook, Twitter, blogs, YouTube, Wikipedia and networking sites such as LinkedIn are all examples of social media. The term covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations.

The Tameside **Social media use: responsible conduct policy** applies to:

- All blogs, wikis, forums, and social networks hosted or sponsored by Tameside;
- Your personal blogs that contain postings about Tameside's business, councillors, employees, residents, customers, or partners;
- Your postings about Tameside's business, councillors, employees, residents, customers, or partners, on any external blogs, wikis, discussion forums, or social networking sites such as Twitter; and
- Your participation in any video related to Tameside's business, councillors, employees, residents, customers, or partners; whether you create a video to post or link to on your blog, you contribute content for a video, or you appear in a video created either by another Tameside employee or by a third party.

WHY DO LOCAL COUNCILS NEED SOCIAL MEDIA?

Local authorities and other public sector agencies are increasingly looking to social media to engage with their audiences for two broad reasons:

1. **The audience is changing** - People also expect to 'talk back' when official bodies communicate with them and they expect that those agencies will in turn respond and do so in appropriate language. New media enables that kind of interaction to happen in a more efficient manner than, for instance, arranging regular public meetings. Also our audience is becoming fragmented and diverse in so many ways. The traditional ways of communicating where budget is invested into a newsletter or another form of mass communication that contains one standard message and assumes this will be effective for everybody is increasingly losing impact. Information needs to be provided in a variety of formats so each target audience can choose how to access it. Photographs can tell a thousand words and videos are very accessible for a wide audience.
2. **Pressure from Central Government** - We all know that public funds are being squeezed from the centre as the focus becomes much tighter on how money is spent, especially on communications. **There** is also an ethos in some areas of Whitehall that egovernment needs to be incentivised and **encouraged**. For these reasons, central government is looking more closely at the degree to which local authorities are using new media to talk to their audiences and this is becoming an increasing factor in the awarding of funds/grants.

APPENDIX 5

WHAT ARE THE BENEFITS OF USING SOCIAL MEDIA?

Used carefully, social media can bring people together over common interests; can be useful for consulting people and getting feedback and publishing information that other media may ignore. However, you must treat social media with respect. Always remember any information or comments you publish on any site (internal or external):

- May stay public for a long time;
- Can be republished on other websites;
- Can be copied, used and amended by others;
- Could be changed to mis-represent what you said; and
- Can attract comments and interest from other people/the media.

Always be aware of the standards, conditions of use and guidelines for posting laid down by the owner of any site or network and make sure you comply with them.

USING SOCIAL MEDIA

This policy applies to you participating in any on-line social media (whether listed here or not), whether privately or as part of your role with the Council and sets out the standards of behaviour the Council expects of all its employees.

You are permitted to use social media from a Council computer at work, provided you comply with the Council's Email, Communications and Internet Acceptable Use Policy and this guidance, and ensure that you use it in a reasonable manner, unless you are specifically using it to undertake Council business e.g. consultation with the public, that you only engage in such social interaction in your own time.

You must make sure any on-line activity does not interfere with your job, your colleagues, your responsibilities and duties as a Council employee, our commitment to customers, is legal and does not bring the Council into disrepute. If you are found to be in breach of any of these policies, then you may face disciplinary action.

STAY LEGAL

You must stay within the law at all times. Be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line just as in any other media. Remember that colleagues and customers may see your online information (e.g. Facebook). Whether you identify yourself as an employee of Tameside Council or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

Never give out personal details like home addresses, phone numbers, financial information or full date of birth to prevent identity theft.

In addition, a person that posts grossly offensive or indecent matter may be found guilty of an offence under the Communications Act 2003 and could be sentenced to up to 6 months imprisonment and/or be fined up to £5,000.

KEEP IT PRIVATE AND DECENT

Remember your obligations to residents, service users, partners, suppliers and colleagues and to protecting the Council's reputation. Never give out details of or divulge dealings with colleagues, customers or partners without their explicit consent. Check with your manager if you are not sure

APPENDIX 5

what is and isn't confidential.

Never make offensive comments about any customer, supplier, partner or any of their employees or your Council colleagues. Don't use ethnic slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace. That could bring the Council into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

Don't pick fights, be the first to correct your mistakes and don't alter previous posts without indicating that you have done so.

Don't be afraid to be yourself, but be considerate about other people's views, especially around 'controversial' topics such as politics and religion. You can challenge without being abusive.

Be credible, be accurate, fair and thorough and make sure you are doing the right thing.

Share useful information that you gain from using social media with others, where appropriate.

Speaking for the Council, you should not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council) unless you are specifically authorised to do so in writing. If you have not been authorised, then please speak to your line manager and the Council's communications team before taking any action.

Remember you are personally liable for what you publish online.

If you are unsure please contact your line senior council manager in the first instance or:

- Sarah Dobson – Assistant Director of Policy, Performance and Communications
- Sandra Stewart – Director of Governance and Pensions (Borough Solicitor/Monitoring Officer)
- Aileen Johnson – Head of Legal Services

GIVING YOUR PERSONAL VIEWS

1. Be professional, responsible and honest and try to add value to any debate. Remember that if people know your **links** with the Council you will be seen as representing the whole Council (even if you are not speaking on our behalf) so be careful.
2. If you are discussing or publishing any information on a website about the Council or council/work related matters, you must make it clear that you are speaking for yourself and not on behalf of Tameside Council. The easiest way to do this is to write in the 'first person' (I think, my view is.) and use a disclaimer, however, this will not protect you from potential disciplinary action should concerns be raised or reported.
4. Be aware that you may attract media interest in you as an individual, so be careful whenever you use social media for personal or business reasons. If you have any doubt, speak to your line manager and the Council's Communications Team before you go on-line.
5. If the media do contact you about something posted on-line, politely ask for their contact details, say you will get back to them and take advice from the Council's Communications Team before any response is given.

GUIDELINES FOR BLOGGING/BLOGGERS

1. Please see the "Keep it private and decent" section
2. If you already have a personal blog or website which shows in any way that you work at Tameside Borough Council you must tell your manager. You should include a simple and visible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of Tameside Borough Council"

APPENDIX 5

3. If you want to start blogging, and your blog/website will say that you work for Tameside Council you should tell your manager and use the disclaimer.
4. If you think something on your blog or website may cause a conflict of interest or have concerns about impartiality or confidentiality, speak to your manager. If in any doubt, don't talk about what you do at work – particularly if you work in sensitive areas (such as social work) or on high profile, controversial projects. The Council has to be seen as honest, transparent, fair and impartial at all times. You must not undermine that.
5. If someone offers to pay you for blogging this could cause a conflict of interest and you must inform your manager.

GUIDELINES FOR SOCIAL NETWORKS, DISCUSSION FORUMS, WIKIS ETC

1. Please see the "Keep it private and decent" section
2. Use your best judgment. Remember that there are always consequences to what you publish.
3. Don't use your work email account or your email or work number in on-line discussions unless you have been authorised to speak for the Council.
4. It is not a good idea to invite customers to become your friends on social networking sites. There may be a conflict of interest, security and privacy issues
5. Make sure any wiki entries, articles or comments are neutral in tone, factual and truthful.
6. Never post rude or offensive comments on any online encyclopaedias
7. Before editing an online encyclopaedia entry about the Council, or any entry which might cause a conflict of interest or adding links, check the house rules of the site. You may also need permission from the relevant wiki editor and your line manager.
8. If you edit online encyclopaedias whilst using a work computer, the source of the correction may be recorded as a Tameside Borough Council IP address. That means it may look as if the Council itself has made the changes. If this is correcting an error about the Council, that's fine – we should be open about our actions. In other circumstances be careful that you do not bring the Council into disrepute through this. If in any doubt, ask the Council's communications team before taking action.
9. We should respond to legitimate criticism with facts but please speak to the Council's communications team for advice before responding; a poor response could make matters worse. Never remove criticism of the Council or derogatory or offensive comments. Report them to the site administrator for them to take action.

GUIDELINES FOR 'MEDIA' SHARING (VIDEO, PHOTOS, PRESENTATIONS)

1. Make sure all video and media is safe to share, does not contain any confidential or derogatory information, and is not protected by any copyright or intellectual property rights.
2. If the content is official Tameside Council content then it must be labelled and tagged as such.
3. Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: "This is my personal work and does not necessarily reflect the views of Tameside Borough Council." Please note that a disclaimer will not protect you from potential disciplinary action should concerns be raised or reported.

USE OF COUNCIL COMPUTER EQUIPMENT

1. Make sure you have read, understood and signed the Council's ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy. This sets out very clearly what you can and cannot do.
2. You must protect the security of our network and information at all times.
3. Do not install any application.
4. Do not open emails from people you don't know and trust, particularly if they have attachments. Do not forward these within the council unless you know they are virus free.
5. Remember online activity can be traced back to the Council and you. Don't do anything online

APPENDIX 5

that breaches the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy and this guidance.

6. Do not reveal any details of the Council's ICT systems and services, including what software we use for email, internet access and virus protection to minimise the risk of malicious attack.
7. If you use secure systems, such as GovConnect email or to process financial transactions, never log onto social networking sites while connected to those systems. If you have used a social networking site, please restart your computer before logging onto the secure system to clear any information in the computer's memory cache.

LEGAL ISSUES

Libel

If you publish an untrue statement about a person which is damaging to their reputation they may take a libel action against you. This will also apply if you allow someone else to publish something libellous on your website if you know about it and don't take prompt action to remove it. A successful libel claim against you will result in an award of damages against you.

Copyright

Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc.) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission in advance. Breach of copyright may result in an award of damages against you.

Data Protection

Avoid publishing the personal data of individuals unless you have their express written permission.

Bias and Pre-determination

If you are involved in planning or licensing application or other quasi-judicial decisions, avoid publishing anything that might suggest you don't have an open mind about a matter you may be involved in determining. If not, the decision runs the risk of being invalidated.

Obscene material

It goes without saying that you should avoid publishing anything that people would consider obscene. Publication of obscene material is a criminal offence.

GUIDELINES FOR MANAGERS

Please make sure you and your employees (including agency workers and contractors) are aware of and working within these guidelines. Please speak to the Assistant Director of Policy, Performance and Communications, Legal, ICT or Human Resources if you have any questions or concerns about interpreting this policy.

Managers are responsible for deciding what is appropriate, bearing in mind concerns about impartiality, confidentiality, conflicts of interest or commercial sensitivity.

If you believe any employee is breaching these guidelines or is spending too much time on the internet/social media), ask ICT to activate internet monitoring for that employee. It is your responsibility as a manager to ensure your employees (including agency workers and consultants) are not abusing Council ICT facilities.

FINALLY....

These guidelines are to protect you and the reputation of the Council. They are not meant to restrict your genuine and work related use of what is an important method of communication and engagement. By its nature though, it is fast and responsive so when a mistake is made it can rapidly get out of control.

If you think social media may help your service you should contact the Assistant Director of Policy, Performance and Communications who can support you and ensure your proposal is supported by the other work being done as part of the corporate communications strategy.

Removable Media Protocol

May 2018

1. Introduction

- 1.1 Tameside Metropolitan Borough Council (the Council) recognises that sometimes there is a business need for information to be temporarily stored outside of the Council's secure network. However, the Council must safeguard information against unauthorised disclosure or loss and also prevent unintended or deliberate adverse impacts to the Council's data and networks.
- 1.2 Note that data accessed via, or held on, a Council issued portable device is covered in the Mobile and Remote Working Protocol.
- 1.3 This protocol aims to ensure that the use of removable media is controlled in order to reduce the risks associated with storing information outside of the Council's secure network.

2. Definitions

- 2.1 Removable media refers to devices that are used to store or transport data. In this protocol the term 'removable media' includes but is not restricted to the following;
 - Optical Disks (CDs, DVDs);
 - USB Memory Sticks (also known as pen drives or flash drives);
 - Memory Cards (including Flash Cards, Smart Cards and Mobile Phone SIM Cards);
 - Media Card Readers;
 - External Hard Drives;
 - MP3 Players;
 - Digital Cameras; and
 - Magnetic/Audio Tapes (including cassettes from Dictaphones and backups).
- 2.2 The following terms are used throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 2018 and the EU General Data Protection Guidelines (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 2018 and the EU General Data Protection Guidelines (GDPR).

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- mental/physical health or condition;
- sexual life;
- a committed or alleged offence; and
- details of the proceedings or the sentence of any court.

Protected Information is any information which is:

- (a) personal/sensitive personal data; or
- (b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

3. Roles and Responsibilities

- 3.1 All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them and must ensure they are not compromised whilst under their control.
- 3.2 Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by informing your line manager and/or Risk and Insurance Manager. Failure to do this could result in a loss having more serious consequences than would otherwise have been the case and could result in fines by the Information Commissioner.
- 3.3 Service areas are responsible for implementing this procedure and must monitor the use of removable media.

4. Use of Removable Media

- 4.1 Removable media (and the associated software/hardware) must only be used if there is a valid business need and with the approval of a Service Unit Manager or above. Use of removable media to transport protected information outside the office environment should be minimised and used as a last resort when no other method of accessing information is available.
- 4.2 Employees should be aware that the use of removable media on the Council's network is logged and monitored and may be subject to audit and inspection.
- 4.3 Any removable media connected to the Council's network that is not encrypted will be 'read only' and no information will be able to be saved onto it. A message will be displayed by the monitoring software. Employees will still be able to view the contents of non-encrypted media.
- 4.4 Files on removable media are automatically scanned for viruses before opening.
- 4.5 As set out in the ICT Security Policy, only encrypted USB memory sticks may be used to store information for which the Council is responsible
- 4.6 Purchases of removable media must be done through the Council's approved ordering system. All removable media devices and any associated software must be supplied, configured and installed by authorised Council personnel or a Council approved third party provider.

5. Security of Information

- 5.1 Removable media must not be used as the sole storage method for business information. Information must be stored on the Council's infrastructure which is secure and appropriately backed up.
- 5.2 Removable media must not be used to store backup data. All data held on the Council's infrastructure is already appropriately backed up.
- 5.3 Information held on removable media should be a short-term measure. Where digital information is transferred it is important to remember that at the point it is transferred, it

becomes a snapshot of the information at that time. Information temporarily held on removable media should be appropriately labelled to ensure that anyone viewing the information can easily identify the version and its content.

- 5.4 In order to minimise physical risk such as loss or theft, all removable media must be stored in an appropriately secure and safe environment when not in use (e.g. locked cupboard or drawer).
- 5.5 Anyone using removable media devices must be able to demonstrate that reasonable care is taken during transportation to avoid damage or loss. Removable media should not be used if direct access to the Council network is available at the remote site.
- 5.6 Council issued removable media must not normally be connected to non-Council owned equipment. Exceptionally, permission may be granted by a Service Unit Manager or above if there is a strong business case for the connection. Advice from ICT Services should be taken to minimise risk of virus infection and data loss.
- 5.7 Passwords needed to access protected information on removable media must only be disclosed to those authorised to access the information held on the media. Passwords must **never** be written down or stored alongside the media.

6. Access to Information

- 6.1 Removable media issued by the Council must only be used for the purposes of Council business. Employees must therefore ensure that any removable media is not accessed by anyone outside the Council without the agreement of a Service Unit Manager.
- 6.2 Protected information must not be transferred to an external third party (e.g. contractor, partner) via removable media unless this is specified within a relevant Information Sharing Agreement. If removable media is to be used, the security arrangements for the media must also be recorded and reflected within the agreement.
- 6.3 Should third parties be granted access to Council information, the third party is required to follow this protocol when they use removable media for the purpose of holding or transferring information.

7. Secure Disposal of Removable Media

- 7.1 It is essential that all removable media is disposed of securely to minimise the risk of the accidental disclosure of sensitive information. For further details on this, refer to the [ICT Equipment Disposal/Recycling Policy](#).
- 7.2 Tapes can be disposed of using the secure tape bins that are provided by Iron Mountain. Discs can be carefully snapped in half or shredded (if your shredder is capable) or cut into pieces.
- 7.3 Removable media devices associated with mobile phones (SIM cards, memory cards etc.) should be returned to Digital Tameside along with the relevant device to ensure any data is removed from the handset before reallocation/disposal.

Mobile and Remote Working Protocol

May 2018

1. Introduction

- 1.1 The Council actively encourages employees to work differently, which will often mean employees access and process information outside the office setting. However, the Council has a duty to safeguard personal and sensitive data and equipment purchased with public funds. In addition, the technology and mobility that make portable devices so useful to employees and the Council can also make them valuable prizes for thieves.
- 1.2 The purpose of this protocol is to recognise the risks associated with mobile and remote working and provide employees with protocols to minimise those risks.
- 1.3 This protocol applies to any access or use outside Council controlled premises of:
 - all Council issued static and portable ICT equipment (see definitions later) and
 - any information held by the Council to which an employee has access because of his or her role within the Council.
- 1.4 All ICT equipment provided to employees by Tameside Metropolitan Borough Council (the Council) remains the property of the Council and must be returned promptly upon request by ICT Services or by managers for audit and inspection, to enable maintenance work to be undertaken, or for removal or disposal.

2. Definitions

- 2.1 The following terms are referenced throughout this document and are defined as follows;

Outside Council controlled premises: includes non-Council locations such as; an employee's home, premises of another organisation and public venues.

Mobile Working: Employees who have the ability to work from multiple locations. Usually accompanied by portable computing equipment, employees can utilise any work space at any given time (including home, office, customer sites, Touch Down Points etc.).

Remote Working: Employees who are able to access information or resources from a remote location. This usually applies to workers who perform their work from home or from an alternative office (e.g. Touch-down Points) on an ad-hoc basis.

Home Working: Employees who are based at home or work from home for all or part of the working week on a regular basis. This would be an agreed arrangement and would necessitate the provision of appropriate equipment, which may be static or portable.

Personal information: is any information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of such information as governed by the Data Protection Act 1998.

Special Category information: (similar to the concept of sensitive personal data under the Data Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

Protected Information is any information which is;

(a) personal/special category (sensitive personal data); or

(b) Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

VPN (Virtual Private Network): refers to a secure network connection that uses the internet to transmit data. It allows employee's access to the Council network out of the office from a Council issued PC/laptop.

Netilla: works in a similar way to a standard VPN but instead of connecting the PC/laptop to the network, it enables a user to connect from any machine as a remote virtual desktop is created. This solution may be replaced by an alternative.

Wi-Fi Hotspot: wireless internet access point in a public location such as a café, retail outlet or hotel.

Personal (Wi-Fi) Hotspot: a wireless internet access point provided by a smartphone.

2.2 In this protocol the term 'portable devices' includes but is not restricted to the following:

- Laptop/slate computers;
- Personal Digital Assistants (PDA's);
- BlackBerry's/Smartphones;
- Mobile phones;
- Text pagers;
- Wireless technologies;
- Digital Cameras; and
- Storage devices including flash memory cards/USB memory sticks.

3. Roles and Responsibilities

3.1 All employees are responsible for the safety and security of portable devices issued to or used by them. Particular care must be taken when moving equipment between sites and storing when not in use.

3.2 Where the Council provides a laptop computer to an employee, it is the responsibility of the employee to ensure that the anti-virus updates are maintained by regularly connecting the device directly to the Council network. This can be done by connecting via a designated Touch-down Point or from their office within a Council building and any automatic update should be downloaded. If employees are not clear on how to check if their anti-virus files are up to date refer to the Service Portal 'how to guides' which can be accessed via the home page of the intranet.

3.3 Employees must not install any software or connect any hardware to a Council owned portable device without the prior permission of the Council. However connection to the following is permitted:

- an external monitor or projector;
- equipment supplied, owned or configured by the Council;
- internet connection via a home router or home broadband modem (wired or wirelessly connected); and
- A printer.

3.4 Employees must not update or change the security configuration of any Council ICT equipment unless advised by ICT Services. This is to prevent potential loss of protected information or damage to a portable device.

3.5 All employees with a Council issued portable device are responsible for the information held on the device. Employees must be aware of their surroundings and take appropriate

measures when viewing information on a portable device to ensure it is not within view of others.

- 3.6 It is the responsibility of individuals to immediately report any actual or suspected breach in information security by informing their line manager and/or the Risk and Insurance Manager. Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. Failure to do this could not only result in reputational damage, but fines could also be imposed by the ICO. The ICO can also fine individuals.
- 3.7 To reduce the risk of unauthorised access whilst working out of the office, protected information must only be stored on Council issued portable devices if they are encrypted (e.g. laptops). Some items like digital cameras cannot be encrypted, however if the contents would be considered to be protected information, the camera (or other storage medium) must be kept securely until it can be transferred to a more secure storage format.

4. Council ICT Equipment and Wi-Fi

- 4.1 To facilitate mobile working and working differently the Council will, by default, issue one laptop or other alternative mobile device to those that need access to the Council's systems. In addition some employees will also be issued a mobile phone, which may be a smartphone, such devices will be authorised by the employee's manager on an individual basis to support the delivery of service provision. All equipment used to store or access any protected information must be supplied, configured and installed by the Council or a Council approved third party provider.
- 4.2 Council provided Wi-Fi is available in most main Council buildings. Staff must use the TMBC_Staff channel. Only Council owned equipment should be connected to this Wi-Fi channel. VPN will still need to be used to make the connection to the Council's network. Two other Wi-Fi channels (public and guest are available and staff owned devices should use the public channel).
- 4.3 Equipment supplied by the Council may only be used by authorised persons. Employees must therefore ensure that the supplied equipment is **not** used by anyone outside the Council. Access to protected information by anyone outside the Council would have to be agreed by a Service Unit Manager. There are instances where permissions may not be required, i.e. showing a Service User information being created about them. However, in this case your Manager should be aware of what you are doing.
- 4.4 ICT equipment may be used for personal purposes by employees so long as it is in accordance with Information Governance Conduct Policy and appropriate supporting policies, protocols, procedures and guidance documents. However, the Council owned equipment must not be used to undertake any private business enterprise.
- 4.5 All faults or requests for upgrades must be logged via the ICT Service Desk (available from the home page of the Staff Portal).

5. Non-Council Equipment

- 5.1 Personal or any other non-Council equipment must not be used to conduct official Council business. This would include employees own smartphones (including iPhones), laptops, iPads/slate PCs, personal desktop computers or internet cafes. However, employees may use remote solutions provided by the Council such as OWA (Outlook Web Application) or Netilla (this solution may be replaced). Under no circumstances should Council data be stored or downloaded onto any non-Council equipment, as it then becomes insecure.
- 5.2 The setting up of personal iPhones or smartphones to receive "push" emails from an employees' own Council Outlook account must **not** be undertaken. Also, Council emails must **not** be forwarded on to a personal email account. Emails sent in these ways exit the

Council's network and are transmitted over an untrusted network. If an email or attachment containing protected information is sent to a personal device/email account, the contents are open to misdirection, interception and corruption and therefore this would be in breach of this protocol.

- 5.3 Employees must not install any Council owned/licensed software onto personal equipment, unless this has been authorised by ICT Services. Any software purchased by the Council is licensed to the Council and any unauthorised use outside of the licence is likely to be a breach of copyright and could result in a prosecution.
- 5.4 Non-Council owned portable devices including mp3 players, iPods/iPhones, cameras and USB memory sticks must **not** be physically connected to Council owned equipment unless expressly authorised by ICT Services. For further information on this, refer to the [Removable Media Protocol](#). The connection of unencrypted devices is logged and monitored by ICT and downloads to these devices are prevented.

6. Physical Security and Insurance

- 6.1 Portable devices issued by the Council are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover. Employees must seek advice from the Risk and Insurance Team before taking any Council owned portable device outside the United Kingdom as the device may not be covered by the Council's normal insurance against loss or theft. There is also the possibility that the device may be confiscated by Airport Security staff, which could result in having to leave them behind, or they may request to see the contents, which could result in a breach of this policy and possibly the law if the device contains protected information.
- 6.2 Employees should be aware of the physical security risks associated with working from a remote office or mobile working location. All protected information (including information stored on portable devices and in paper files) must not be left where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight so that visitors or family members do not have access. Unauthorised disclosure of protected information is a breach of this protocol and the law.
- 6.3 Council equipment and protected information must be kept safely and securely at all times. When equipment/protected information are at home, employees must:
 - ensure that only the employee has access to the equipment/information;
 - ensure that the equipment/information is safely and securely locked away when not being used;
 - prevent access to the Council equipment and protected information, by family members and visitors; and
 - ensure that any telephone conversations discussing protected information cannot be overheard.

These precautions are necessary to reduce the risk of unauthorised persons listening to or viewing Council information.

- 6.4 Employees who regularly work at home must have a suitable workstation where these issues have been considered. In order to prevent a potential breach, documents should be collected from printers as soon as they are produced and not left where they can be casually read.

7. Use of Information Out of the Office

- 7.1 All Council supplied laptops (and all USB memory sticks authorised for use by the Council) are encrypted and so provide a secure method in which to save information when necessary. However, whilst this is likely to prevent unauthorised access to the information,

it does not protect the information against loss. Therefore documents and files should be saved on shared drives to prevent any loss of information. Master copies of information must never be held on a portable device on anything other than a temporary basis. Once the temporary information is no longer required on the portable device it must be deleted.

- 7.2 It is also possible to setup folders so that they can be worked on off-line, which means there is a local copy of the data. This will allow a user to work out of the office without access to the Council network. However only a limited number of folders should be made available off-line in order to avoid performance issues on the laptop. In addition folders that contain personal data should only ever be made available off-line on a temporary basis.
- 7.3 All Council supplied laptops are provided with software to connect to a Virtual Private (VPN) network to allow secure access to the Council Network. VPN software will NOT be installed on non-Council equipment as this is a security risk. Most employees are issued with a laptop but if you are using a static computer and you need remote access to the council network please submit a request to exchange your computer with a laptop. In some rare circumstances, information may need to be accessed via an authorised mobile device or transferred to a form of removable media to assist mobile and remote working. If the information is of a protected nature, it is essential that the media or device has been issued by the Council and is encrypted and your line manager **must** be aware of what you are doing.
- 7.4 When working out of the office, employees should avoid using Wi-Fi Hotspots or free Wi-Fi connections provided by retail outlets, coffee shops and the like. Even when connected via the Council's VPN, hackers could still intercept transmissions potentially revealing protected information or password and login details. Individuals are required to assess the risks based on the data they work with. Those that work with personal and sensitive data should not use such facilities and instead use the personal Wi-Fi hotspot facility on their Council provided smartphone (also using the VPN software on their laptop). Others are permitted to use these facilities but must never give any information about their Council email account or passwords. Employees must refer to their manager or the Risk and Insurance Team if they are uncertain. The only exception to this would be a private network that requires a password to access, for example Wi-Fi at another Local Authority building, or at a business or academic premises. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.
- 7.5 Some services may require physical documentation (e.g. paper files) to be removed from the office to assist with mobile and remote working. If this is the case, a booking out system should be in place which meets the requirements of the service. This is to ensure that your Manager is aware of the movement of information within their service, as if a loss occurs they will need to provide assurance they were controlling their information adequately.
- 7.6 Arrangements must be made to properly dispose of any protected information used out of the office in order to prevent unauthorised access. To do this any information that would qualify as being personal or sensitive must be returned to the Council office and disposed of in the blue Iron Mountain security bins or shredded.

Access and Security Protocol

May 2018

1. Policy Statement

- 1.1 Tameside Metropolitan Borough Council (The Council) will establish specific requirements for protecting information and information systems against unauthorised access.
- 1.2 The Council will effectively communicate the need for information and information system access control.

2. Introduction

- 2.1 Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Council which must be managed with care.
- 2.2 Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.
- 2.3 Formal procedures must control how access to information is granted and how such access is changed.
- 2.4 This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. Scope

- 3.1 This Access and Security Protocol outlines the framework for the management of Access Control within the Council.
- 3.2 The Access and Security Protocol applies to all employees (including system support staff with access to privileged administrative passwords), Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any Information Systems or information for Council purposes.
- 3.3 Access control rules and procedures are required to regulate who can access the Council's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council information in any format, and on any device.

4. User Access Management

4.1 Access Control

- 4.1.1 Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by the Council.
- 4.1.2 Each user must be allocated access rights and permissions to computer systems and data that:
 - Are commensurate with the tasks they are expected to perform.
 - Have a unique login that is not shared with or disclosed to any other user.
 - Have an associated unique password that is requested at each new login.

- 4.1.3 User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

4.2 User Registration

- 4.2.1 A request for access to the Council's computer systems must first be submitted to the ICT Service Desk for approval. Applications for access must only be submitted if approval has been granted from the line manager
- 4.2.2 When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT Service Desk

4.3 User Responsibilities

- 4.3.1 It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:
- Following the Password Policy Statements outlined in Section 10.
 - Ensuring that any PC they are using that is left unattended is locked or logged out.
 - Leaving nothing on display that may contain access information such as login names and passwords.
 - Informing the IT Service Desk of any changes to their role and access requirements.

5. Network Access Control

- 5.1 The use of modems on non-Council owned computers connected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from ICT before connecting any equipment to the Council's network.

6. User Authentication for External Connections

- 6.1 Where remote access to the Council network is required, an application must be made via the ICT Service Desk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example encrypted devices and password protection. For further information please refer to the Mobile and Remote Working Protocol.

7. Supplier's Remote Access to the Council Network

- 7.1 Partner agencies or Third party suppliers must not be given details of how to access the Council's network without permission from ICT within a business case. Any changes to supplier's connections must be immediately sent to the ICT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by ICT with assurances from the SIRO.
- 7.2 Partners or Third party suppliers must contact the ICT before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

8. Operating System Access Control

- 8.1 Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (4) and the Password section (10) must be applied. The login procedure must also be protected by:
- Not displaying any previous login information e.g. username.
 - Limiting the number of unsuccessful attempts and locking the account if exceeded.
 - The password characters being hidden by symbols.
 - Displaying a general warning notice that only authorised users are allowed.
- 8.2 All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).
- 8.3 System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

9. Application and Information Access

- 9.1 Access within software applications must be restricted using the security features built into the individual product. The manager of the software application is responsible for granting access to the information within the system. The access must:
- Be compliant with the User Access Management section (4) and the Password section (10).
 - Be separated into clearly defined roles.
 - Give the appropriate level of access required for the role of the user.
 - Be unable to be overridden (with the admin settings removed or hidden from the user).
 - Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
 - Be logged and auditable.

10. Password Security

10.1 Choosing Passwords

- 10.1.1 Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.
- 10.1.2 A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

10.2 Weak and Strong Passwords

- 10.2.1 A *weak* password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.
- 10.2.2 A *strong* password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.
- 10.2.3 Everyone must use strong passwords with a minimum standard of:

- A minimum of seven characters.
- Contain a mix of alpha and numeric, with at least three non-alphabetic characters (i.e. numbers and/or symbols).
- More complex than a single word (such passwords are easier for hackers to crack).
- For further password guidance, [click here](#) to visit the IT Service Portal and type 'password' in the search box.

10.3 Protecting Passwords

10.3.1 It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different TMBC systems.
- Do not use the same password for systems inside and outside of work.

10.4 Changing Passwords

10.4.1 All user-level passwords must be changed at a maximum of every 42 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the SUM or Information Asset Owner.

10.4.2 Users **must not** reuse the same password within 20 password changes

10.5 System Administration Standards

10.5.1 The password administration process for individual Council systems is well-documented and available to designated individuals.

10.5.2 All Council ICT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users (i.e. no generic accounts).
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

11. Compliance

- 11.1 This Access and Security Protocol takes into consideration all applicable statutory, regulatory and contractual security requirements.
- 11.2 It is the responsibility of Managers to exercise appropriate controls to minimise the risk of unauthorised access and where misuse is suspected to report it via the Incident Reporting Procedure process, using the form on the Information Governance page.
- 11.3 It is the responsibility of all employees to ensure that they have read and comply with the conditions laid out in this protocol.

- 11.4 Non-compliance with this protocol could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.
- 11.5 If any user is found to have breached this protocol, they may be subject to the Council's Disciplinary Procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
- 11.6 If you do not understand the implications of this protocol or how it may apply to you, please seek advice from the Risk and Insurance Team or the Council's ICT Security Officer. Manager.

12. References

- 12.1 This Access Control Protocol should be read in conjunction with the overall [Information Governance Policy and Conduct Policy](#) and related sub documents
- 12.2 The following TMBC policy documents are directly relevant to this policy, and are referenced within this document:
- [Mobile and Remote Working Protocol.](#)
 - [Incident Reporting Procedure.](#)

Information Security Incident Reporting Procedure/Practice Note

May 2018

1. Introduction

- 1.1 Tameside Metropolitan Borough Council (the Council) will ensure that it reacts appropriately to any actual or suspected incidents relating to electronic or paper based information systems within the custody or control of the Council or its contractual third parties.
- 1.2 This procedure must be applied as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident.
- 1.3 All incidents, irrespective of scale, must be reported using the incident management procedure to allow for lessons to be learned and to improve information handling procedures and the incident response process.

2. Definitions

- 2.1 The following terms are used throughout this document and are defined as follows;

Information Security Incident: is defined as an adverse event that has caused or has the potential to cause damage to the Council's assets, reputation, personnel and/or citizens.

An information security incident can occur when there is an actual or potential loss of information or when information is discovered (e.g. USB memory stick/paper files found or handed in).

On some occasions, an information security incident will include personal data and will entail a breach of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Examples of Information Security Incidents are provided at **Appendix 1**.

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Special Category information: (similar to the concept of sensitive personal data under the Data Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

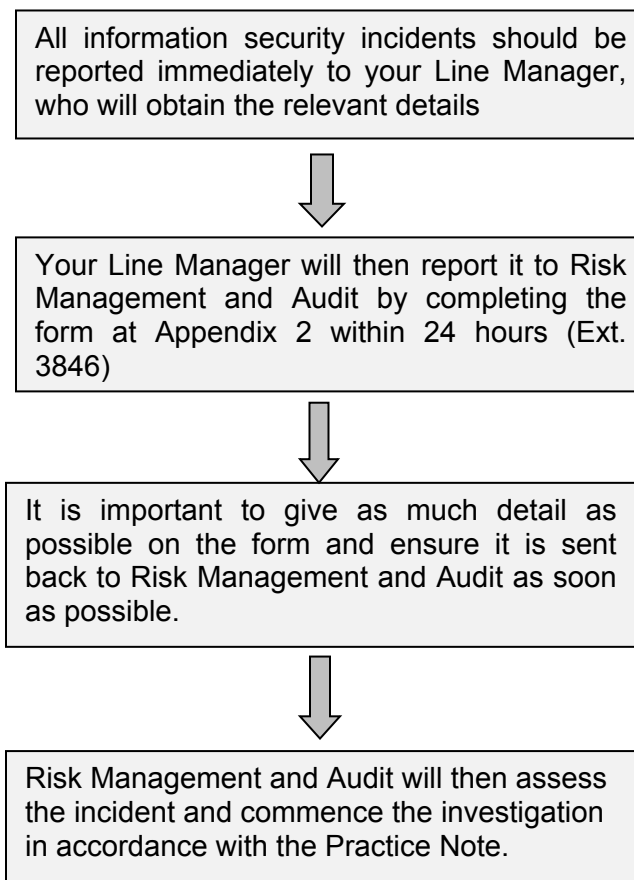
Protected Information is any information which is;

- (a) personal/special category (sensitive personal data) or
- (b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled manner.

3. Roles and Responsibilities

- 3.1 All employees must understand and adopt the use of this procedure and are responsible for the safe and secure use of Council information and systems.
- 3.2 All employees have a duty to report actual or suspected information security incidents and to fully support an investigation. Failure to report an Information Security Incident immediately or within 24 hours at the latest of discovery could result in disciplinary action.

4. Reporting an Incident



Note: If information has been discovered in any format (e.g. Memory Stick), it is important that you do not do anything with the information unless advised to do so by Risk Management and Audit. Report as you would normally through the information security incident procedure outlined above.

5. Incident Investigation

5.1 Initial Response

- 5.1.1 Once the Information Security Incident Form has been received an evaluation can take place to identify if, there may be a need for immediate action in order to limit the damage from the incident and recover any losses. Action may also be needed to prevent another incident with similar circumstances whilst the investigation is taking place. This may include action taken to:
- prevent any further unauthorised access;
 - secure any affected buildings (i.e. changing locks, access codes etc.);
 - recover any equipment or physical information;
 - restore lost or damaged data by using backups; or
 - prevent a further incident relating to the same information (e.g. an attempt to use stolen data to access accounts or services)
- 5.1.2 The Risk Management and Audit Team will determine if any immediate action needs to be taken based on the details provided and will notify the relevant persons.

5.2 Investigation Process

- 5.2.1 Risk Management and Audit at this stage will review the incident and consult with other information governance specialists in the Council where appropriate before an investigation will commence. The investigation may involve the following:-
- Senior Information Risk Owner (SIRO);
 - Data Protection Officer/Data Controller;
 - Service Director or a representative for the relevant part of the directorate;
 - Line Manager of person who has caused the incident;
 - Head of Human Resources or a representative;
 - Head of ICT/ICT Security Officer;
 - Head of Media, Marketing and Communications or a representative;
 - Facilities Management; and
 - Caldicott Guardian
- 5.2.2 Depending on the type and seriousness of the incident, the police may be involved and the employee/s suspended from the work place.
- 5.2.3 The Risk Management and Audit Team will use the checklist outlined at **Appendix 3** along with any other information required, to investigate the incident and will record any key findings from this point forward.
- 5.2.4 Once the investigation is completed, a summary of the incident will be presented to Senior Management for evaluation and signing off.

6. Evaluation

- 6.1 A consistent approach to dealing with all security incidents must be maintained across the Council and each incident must be evaluated. It is important not only to evaluate the causes of the incident but also the effectiveness of the response to it.

6.2 The evaluation of the information security incident will include some of the following questions:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?

6.3 Assessment of Ongoing Risk

6.3.1 Any identified weaknesses or vulnerabilities must be accurately assessed in order to mitigate the ongoing risks to information. In order to make an assessment, the following factors will be considered:

- Type of data involved;
- Number of people that could be affected;
- Impact on individuals;
- Protections in place (e.g. encryption);
- Likelihood of the identified risk;
- Possible consequences for the Council's reputation; and
- Potential risks to public health or safety.

7. Actions

7.1 Once the investigation and the evaluation of the incident is concluded, any identified actions will be approved by Senior Management and implemented appropriately throughout the Service involved or if required the whole organisation.

7.2 Notification

7.2.1 Depending on the incident there may be legal, contractual or sector specific requirements to notify various parties. Notification may assist in security improvements and implementation, as well as risk mitigation.

7.2.2 The following parties may need to be notified following an Information Security Incident:

- **Information Commissioner's Office (ICO)**
 - Does the incident involve personal data? If so:
 - Does the type and extent of the incident trigger notification?

We have to notify the ICO **within 72 Hours** of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

- **Individuals**
 - Notification to the data subjects involved maybe required where the incident is likely to result in a high risk to their rights and freedoms.
- **Other Agencies**(not an exhaustive list)
 - Identity and Passport Service
 - Her Majesty's Revenue and Customs (HMRC)
 - Bank or credit card companies

- Trade Unions

7.2.3 Notification to any parties will be determined and agreed by Legal Services and Senior Management as part of the evaluation of an incident.

7.3 Disciplinary Action

7.3.1 It may be deemed necessary to follow the disciplinary procedure for any employee(s) involved in an information incident.

7.4 Policy and Procedural Changes

7.3.1 There may be a need to implement policy and procedural changes as a result of an Information Security Incident.

7.5 Employee Notification and Training

7.3.2 There may be a requirement to notify employees of policy and procedural changes and to repeat, extend or revise training following an Information Security Incident.

Examples of Information Security Incidents

Examples of Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Computer infected by a Virus or other malware
- Sending a sensitive e-mail to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature
- Receiving unsolicited mail which requires you to enter personal data
- Hacking attacks which intend to gain information from computers and/or systems using a number of methods (e.g. phishing, password cracking, key logging)
- Changes to information or data or system hardware, firmware, or software characteristics without appropriate authority or the Council's knowledge, instruction, or consent
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it (including information which could assist in gaining access to council data e.g. a password)
- Use of unapproved or unlicensed software on Council equipment
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password)
- Writing down your password and leaving it on display / somewhere easy to find
- Printing or copying confidential information and not storing it correctly or confidentially
- Theft / loss of a hard copy file
- Theft / loss of any Council computer equipment on which information is stored
- Discovery of hard copy information or electronic media on which information may be stored (e.g. disc or USB memory stick)
- Unwanted disruption or denial of service to a system which may cause an adverse effect to the information held within
- Equipment failure that results in the loss of or damage to information
- Unforeseen circumstances such as fire or flood that damages information or areas where information is stored
- Posting inappropriate comments or material online (including on social networks)

Information Security Incident Reporting Form

Please send the completed form to the Head of Risk Management and Audit and DO NOT take any further action unless advised. The incident will be investigated and where appropriate a report issued for action.

Directorate/Service Area	
Assistant Director	
Service Unit Manager/Line Manager	
Employee Reporting Incident	
Person Responsible for Incident	
Date/Time of Incident	
Type of Data/Information Involved - (Paper/Email/Letter/Electronic Data)	

Details of Incident:	
Describe in detail how the incident has occurred?	
Did the employee self-report the incident?	
Are there any mitigating circumstances put forward by the employee?	
Outline what data/information is involved? e.g. <ul style="list-style-type: none"> • Health or Social Care? • Financial (e.g. bank details)? • Personally Identifiable Information (e.g. Name, Address, NI Number)? • Special category information (e.g. race, religion, health) 	
Please attach a copy of the letter/document inadvertently disclosed.	
Approximately how many people have been affected?	
Is the incident a one off or has more than one incident occurred over a period of time? Please provide details and copies of letters etc.	
Has there been any media coverage of the incident?	
Are any other partners involved?	
Has the document/file/data/information been recovered?	
Immediate Action Taken:	
Have you taken any action to reduce the effect on the data subjects involved? If so please provide details:	

Signed:

Date:

Job Title:

Return to: Head of Risk Management and Audit – Wendy Poole

Information Security Incident Investigation Checklist

The following questions may be asked during the investigation process.

How was the incident discovered?

What type of data is involved?

- Health or Social Care?
- Financial (e.g. bank details)?
- Personally Identifiable Information (e.g. address, NI number)?

Whose data is involved?

- Service users, patients or customers?
- Councillors?
- Council employees?
- Suppliers or partners?

How many people could be affected by the incident?

What could the information be used for?

What impact has the incident on?

- **Data Subjects:**
 - Physical harm
 - Mental anguish/distress
 - Reputation/embarrassment
 - Financial loss
 - Identity theft
 - Breach/loss of confidence
- **Employees:**
 - Embarrassment
 - Mental anguish on employees involved
 - Interruption of service to clients
 - Loss of confidence in service provision
- **The Council:**
 - Embarrassment/reputational damage
 - Breach/loss of public confidence
 - Press involvement
 - Potential legal action

What immediate action has been taken to recover the information?

Had the incident been identified as a risk prior to its occurrence?

What controls were in place to prevent the incident?

How likely is the incident to occur again?

Are the relevant employees aware of current policies and procedures?

Did the incident involve deliberate or reckless behaviour by an employee?

Please note that this list is not exhaustive. Other questions may be asked depending on the nature of the incident.

Information Security Incident Reporting Procedure – Practice note

May 2018

Incident Reporting Procedure – Practice Note

This practice note is to be used in conjunction with the Incident Reporting Procedure.

1. Incident Reporting

- 1.1 All employees have a duty to report actual or suspected information incidents immediately.
- 1.2 Disciplinary action will be automatically invoked if an incident comes to light by way of a complaint or referral from the ICO where it had not been reported internally.

2. Initial Response

- 1.1 Once the Incident Reporting Form has been received by your manager it will be passed to Risk Management and Audit who will determine if:
 - Any immediate action is needed in order to limit the damage from the incident and recover any losses.
 - Any action is needed to prevent another incident with similar circumstances from occurring. This may include action taken to:
 - prevent any further unauthorised access
 - secure any affected buildings (i.e. changing locks, access codes etc.)
 - recover any equipment or physical information
 - restore lost or damaged data by using backups
 - prevent a further incident relating to the same information (e.g. an attempt to use stolen data to access accounts or services)
 - The incident needs to be reported to the ICO.

2. Investigation Process

- 2.1 Risk Management and Audit will review the Incident Reporting Form in conjunction with People and Workforce Development and Legal Services (where appropriate) and based on the criteria below determine whether a formal investigation needs to be undertaken.
- 2.2 Assessment Criteria:
 - Contained to less than 5 individuals
 - First incident by employee
 - Nature of information released
 - Information recovered
 - Limited impact on individual (E.G. No safeguarding issues)
 - Any mitigating circumstances put forward
 - Did the individual self-report the incident
- 2.3 If the answer is “Yes” to all the above criteria then an informal interview will be held with the employee to discuss the incident to determine if any corrective action is needed to processes and procedures or whether more training is needed. The disciplinary process will not be invoked. A memo will then be issued summarising the key points and circulated to:
 - Data Protection Officer
 - Director
 - Assistant Executive Director

- Service Unit Manager
- Monitoring Officer
- Caldicott Guardian (Where appropriate)
- Senior Information Risk Owner (SIRO)
- Head of HR Operations and Workforce Strategy

2.4 A standard outcome letter will be sent to the employee (copied to manager) from Risk Management and Audit at the conclusion of the informal interview explaining that if any further incidents occur they may be subject to disciplinary action?

2.5 If the answer is “No” to any of the above criteria then a further assessment of the incident will be undertaken to determine if a formal investigation is required as part of the Council’s Disciplinary Procedure. The list below details some further areas for consideration:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?
- Did the individual self-report the incident?

Appendix 3 in the Incident Reporting Procedure contains more questions for consideration.

2.6 If an incident is reported to the ICO then a formal investigation will be required.

2.7 The formal investigation will be conducted in conjunction with People and workforce Development and will follow the Council’s Disciplinary Procedure. At the conclusion of the investigation Risk Management and Audit will issue a report which will be circulated to:

- Data Protection Officer
- Director
- Assistant Executive Director
- Service Unit Manager
- Monitoring Officer
- Caldicott Guardian (Where appropriate)
- Senior Information Risk Owner (SIRO)
- Head of HR Operations and Workforce Strategy

2.8 Depending on the type and seriousness of the incident, the police may be involved and the employee/s suspended from the work place.

2.9 Informing the data subject(s) involved will need to be determined on a case by case basis in conjunction with Legal Services.

Secure/Clear Desk Procedure

May 2018

1. Introduction

- 1.1 A secure/clear desk is essential to mitigate the risks associated with unauthorised access to Tameside Metropolitan Borough Council's (the Council) information. Applying a secure/clear desk procedure reduces the threat of a security breach as information is kept out of sight.
- 1.2 In order to enable employees to work in a more efficient way, the Council is moving towards a shared working environment and there may be a requirement for an employee to work in different locations or for more than one employee to use a desk or a work station. To facilitate such a change in the working environment, a secure/clear desk procedure is essential to ensure that each work space is productive and protected.
- 1.3 This procedure applies to all information of a personal, confidential or sensitive nature. It also takes into account any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point).

2. Definitions

- 2.1 The following terms are used throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR).

Special Category information: (similar to the concept of sensitive personal data under the Data Protection Act 1998). This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of:-

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health;
- sex life; or
- sexual orientation.

Protected information is any information which is;

- (a) personal/special category (sensitive personal information) *or*
- (b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

3. Roles and Responsibilities

- 3.1 All employees must ensure that their work environment follows the secure/clear desk procedure.
- 3.2 It is the responsibility of individual services to implement this procedure and monitor work areas.
- 3.3 It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by following the [Incident Reporting Procedure](#).

4. Secure/Clear Desk Procedure

- 4.1 The secure/clear desk procedure is required to ensure that all protected information is held securely at all times. Information identified as protected must not be left out on desks when unattended to prevent information being read by unauthorised parties.
- 4.2 For periods away from your desk, working papers containing protected information must be placed out of sight and, where necessary, in a locked cupboard or drawer. Information that is not protected (i.e. contains no personal, sensitive or confidential data) may be left tidily on desks.
- 4.3 At the end of each day, all information should be stored in locked cupboards/drawers or within a locked room. Protected information must be stored away securely and not left on view. Computer equipment must be shut down and where appropriate laptops should be taken with you.
- 4.4 Protected information should not be left lying on printers, photocopiers or fax machines, even if they are in a locked room. These should all be checked at the end of the working day and any papers stored securely overnight.
- 4.5 Whenever you leave your desk and your PC/Laptop is switched on, you should lock your computer by pressing Ctrl, Alt and Delete and then confirm that you wish to lock your workstation.
- 4.6 If you are working on protected information and you have a visitor to your desk who does not have a need to know that information, ensure that you lock your screen or ensure that the information is not visible to them to prevent the contents being read. Even the knowledge that a file is held on a person can be considered an information breach.
- 4.7 All waste paper which contains protected information must be disposed of appropriately (i.e. shredded or placed in the Blue Locked bins). Under no circumstances should this type of waste paper be thrown away in normal rubbish or recycling bins. For further information on the secure disposal of information see the [Retention and Disposal Guidelines/Schedule](#).
- 4.8 Protected information should not be stored in boxes and/or folders on top of any furniture (cabinets etc). This is insecure as they can still be accessed.
- 4.9 When using a hot desk or touch down point, you must consider the length of time you may be away from a desk (to attend a meeting, go for lunch, etc.). It is important to think about the security of your surroundings and secure any protected information where necessary.

This page is intentionally left blank

The Golden Rules

May 2018

Information Security– Golden Rules

Information is a valuable asset. The Council has a duty and responsibility to protect it. This responsibility is placed on the Council by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) and monitored and regulated by the Information Commissioner's Office.

The Information Commissioner has powers to impose monetary penalty notices for up to €20,000,000 for breaches of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR), along with having the authority to carry out assessments of organisations to ensure their processes follow good practice. The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines 2017 by the Public Services Network. The Council wants to comply with these guidelines to ensure good practice is being followed. The Council needs to ensure that everyone uses and manages information assets and information systems in an effective, efficient, and ethical manner.

The objective is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. The Council is committed to protecting information through preserving:

Confidentiality - Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

Integrity - Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability - Being accessible and useable on demand by an authorised individual, entity or process.

It is essential that you understand your data protection and security obligations and that every day business practice helps foster an organisation wide security-aware culture embracing good data/information handling behaviours.

These Golden Rules aim to help you:

- safeguard the Council's valuable information assets, systems and equipment;
- use information assets responsibly within the framework of the law;
- make sure you understand the corporate policies with which you must comply; and
- signpost the mandatory corporate on-line training you must undertake.

All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework of policies, procedures, standards and guidance and also ensure you follow any localised business specific data handling requirements.

Protected Information is any information which is:-

- personal/sensitive personal information; or
- confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

Personal information: is any personal data as defined by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR). Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of

personal information held by it as governed by the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR).

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court

You are personally accountable for safeguarding and using the Council's information assets responsibly and appropriately. Make sure you understand the rules for handling the information, systems and equipment in your care and stick to those rules rigidly.

[Rule 1 – Respecting “need to know” principles](#)

[Rule 2 – Avoiding inappropriate disclosure](#)

[Rule 3 – Keeping your passwords safe](#)

[Rule 4 – Storing data securely](#)

[Rule 5 – Working securely in the office](#)

[Rule 6 – Working securely on the move and away from the office](#)

[Rule 7 – Working safely on line](#)

[Rule 8 – Sending protected information securely](#)

[Rule 9 – Disposing of protected information securely](#)

[Rule 10 – Undertaking mandatory on line training](#)

[Rule 11 – Reporting incidents](#)

[Rule 12 – Preventing security incidents](#)

Rule 1: Respecting “need to know” principles

- Only access protected information if it is part of your job and you have a legitimate business need to know.
- Never access protected information for personal interest or gain.

- If you need protected information 'owned' by another business area to do your job, make sure you are authorised to ask for it, you only ask for the minimum necessary for the required purpose and, you are clear why you are entitled to it.

Rule 2: Avoid inappropriate disclosure

- Before disclosing protected information to an external third party always ask yourself "*is this request legitimate?*" and verify that the requester is who they say they are.
- Always make certain you have the legal authority, including the legal power to disclose the information.
- Check whether the purpose could be satisfied with anonymised rather than protected information.
- Keep a documented audit trail of all ad hoc disclosures.
- If you are unsure of the rules, check with your manager, Legal Services or Risk Management and Audit Services.
- Check whether you need consent to share or if sharing is governed by a legal gateway.

Rule 3: Keeping your passwords safe

- Protect passwords at all times.
- This applies to all passwords enabling access to data and to the Council's network, business systems, email and the internet.
- Avoid writing your password down and if you have to, don't leave it in obvious places such as under your keyboard, next to your monitor or other easily searchable places.
- Ensure that your password is sufficiently complex that you can remember it but it cannot easily be guessed by others.
- Immediately change your password if you suspect it may have been compromised.
- Please refer to the ICT Freshdesk.

Rule 4: Entering and storing data securely

- Enter data accurately and completely.
- Physical files containing protected information must be locked away securely.
- Always save electronic files on the Council's network drives and do not keep the information on your local computer hard drive.
- Remember the secure network is automatically backed up and remains available even if your computer fails.
- If you are working away from the office, access to view or amend data should be via a secure remote connection to Tameside's network.
- If this is not possible and permission is granted to create or store protected information on encrypted portable devices or removable media, this must be the minimum necessary for the approved business purpose.
- The authorised user is responsible for ensuring that unique data held on encrypted devices is regularly backed up to the Council's secure network.
- Information assets must be managed in accordance with the retention and disposal guidelines. Once no longer required for legal, regulatory or business purposes, information should be securely disposed of in line with the retention and disposal schedules for your service area.
- Only retain the minimum necessary information for the minimum period of time.

Rule 5: Work securely in the office

- Never leave protected information or other valuable assets out on your desk when you are not around.
- Remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else.

- When sending information by post check that you have only included the correct documents, especially if collected from shared printers/copiers.
- Lock your work station, log off at the end of the day and switch off your screen.
- Lock windows, offices and conference rooms containing physical records and computer equipment whenever the area is unoccupied.
- Wear your pass when you are in Tameside buildings, remove it and keep it safe when you leave.
- Challenge anybody you see in your building who is not wearing an appropriate security pass.

Rule 6: Work securely on the move and away from the office

- If you are authorised to carry protected information in paper files and/or on encrypted devices beyond your secure workplace keep your laptop, mobile device, and official papers with you at all times and take reasonable precautions based on the environment you are in.
- Ensure that you:
 - comply with local physical file tracking procedures;
 - make sure your laptop is protected with encryption software;
 - avoid “*shoulder surfers*” in public places viewing your screen or confidential business conversations being overheard;
 - do not leave protected information or equipment in an unattended vehicle (unless securely locked in the boot); and
 - limit the risk of valuable information or equipment being lost or stolen (i.e. by not taking council resources to places where they are at risk of being stolen).
- Always ask yourself the question “*Do I really need to take protected information out of the office?*” The best way to prevent theft or accidental data loss is to leave it safely on Council premises.
- Only take the minimum necessary paper records with you (rather than the whole file).
- Do not let unauthorised people, including family members, use or view valuable council resources.
- If you have encrypted equipment and protected information in physical files overnight in your home, reduce the risk by ensuring that the unencrypted physical files are locked away separately.

Rule 7: Working safely on line

- Make sure you understand the Council’s internet and email policies.
- Never open an email from sources you do not know and trust.
- Always report any unusual email messages or suspicious attachments or links especially in unsolicited emails.
- Never use non-Tameside email accounts to send or receive protected information.
- Follow the ICT Security Policy.

Rule 8: Sending protected information securely

- Be diligent when sending letters, addressing envelopes, choosing fax numbers and email addresses to prevent errors and misdirection.
- Try to limit the harm which might be caused if something goes wrong by thinking about whether you need to reiterate sensitive details (i.e. identifiers or bank account numbers the recipient has previously supplied) and send only what you absolutely need to send and no more.
- Do not send protected information by external email **UNLESS**:
 - You have a GCSX account and are sending it securely to another GCSX mail account (or any of the other secure government networks); **or** You are sending it in an attachment, using strong password protection and encryption software such as Egress Switch.

- If you are sending protected information by internal email, within the Council's secure network, always check you have addressed the email correctly to avoid sending it to the wrong person.
- Do not send protected information to a generic mail address unless appropriate and you actually know the mail address relates only to a Tameside internal mail account.
- Only transport protected information on removable media (cameras, DVDs, memory sticks etc.) if you are using Council supplied devices and obtain assurance that the device or the information stored on it, is encrypted to recognised industry standards.

Rule 9: Disposing of protected information securely

All resources containing protected information must be disposed of securely. This applies to protected information held in various formats including:

- paper records (e.g. printed notes, assessments, correspondence or reports).
- electronically stored on encrypted laptops and other portable devices.
- stored on approved removable media, for example writable CDs, writable DVDs, external hard drives, audio and video tapes.

Portable laptops that are no longer required must be returned to ICT enabling the hard drive to be permanently erased with specialist software before disposal or recycling to another business area.

Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Service for secure disposal.

Confidential paper waste must be kept separate from ordinary paper waste and protected from accidental loss, damage or unauthorised access until its final removal/disposal. Follow the minimum standards in the Council's corporate policy for disposing of waste, as supplemented by locally agreed business operating procedures.

Particular care must be exercised during office relocations and moves to ensure that all confidential paper waste and non-required ICT equipment is disposed of properly.

Rule 10: Training

On line Data Protection and Information Governance training is available via the MeLearning portal and is mandatory for all staff.

A Data Protection video produced by the ICO is available on the Information Governance pages on the Staff Portal as an additional resource.

Specific workshops are available on request. Please contact the Risk Management and Insurance team to discuss.

Further guidance and resources are available on the Staff Portal under [Information Governance](#).

Rule 11: Reporting Incidents

You must always report actual or suspected security violations, problems or vulnerabilities to the ICT Security Officer (Ext. 2773) as soon as possible.

If the incident or near miss, involves the loss, theft or unauthorised disclosure of protected information it must be reported immediately via the Incident Reporting Procedure.

Delaying reporting an incident makes it more difficult to solve the problem. Report it straight away so your manager, ICT, Legal Services and Risk Management and Audit are able to act quickly and get any expert advice they may need.

If an incident is reportable to the ICO it needs to be completed within 72 hours.

Rule 12 – Preventing security incidents

Remember good data security is in your interest too.

Security breaches caused by deliberate, negligent or reckless behaviour could result in disciplinary action, dismissal and even give rise to personal fines (up to £50,000) and criminal offences. Make sure you observe the Council's confidentiality, data protection and information governance rules. This will help avoid misuse, unauthorised disclosure, modification, loss or theft of protected information assets which can harm individuals, commercial/partner organisations and/or the reputation of the Council.

Work Securely

These Golden Rules apply whether you are in the office, working remotely or on the move. They aim to ensure you play your part in ensuring our information and information systems are not compromised. Be security alert at all times and do not exceed your access privileges or authority.

This page is intentionally left blank

Subject Access Request Guidance

May 2018

CONTENTS

1. [SAR Process Flowchart](#)
 2. [Introduction](#)
 3. [Scope Of This Guidance](#)
 4. [The Right Of Subject Access](#)
 5. [Roles And Responsibilities](#)
 6. [What Makes A Valid SAR Request](#)
 7. [Requests For Information About Children](#)
 8. [Handling The SAR](#)
 9. [Requests Involving Third Party Data](#)
 10. [Exemptions](#)
 11. [Complaints About Subject Access](#)
- [Appendix One: Identifying Personal Data](#)
- [Appendix Two: Schedule of Disclosed Documents](#)

1. SAR PROCESS FLOWCHART

A written request for records has been received. Is this a subject access request (SAR)? If yes, this needs to go to the central SAR team.

Any written request by an individual asking for their personal information is a subject access request. You can choose to deal with it in one of two ways: as a routine enquiry, or more formally. If you can, treat requests that are easily dealt with as routine matters, in the normal course of business; for example: What is my customer reference number?

However some need to be treated formally: Please send me a copy of my staff records.



Does the requester have sufficient authority to access the records i.e. they are the subject, they have parental responsibility, they are instructed / have authority to act on the subjects behalf?



Have we had sight of sufficient ID and received the relevant fee?



DAY 1
Log request and pass onto relevant SUM to be delegated to the team / person responsible for dealing with SARs



DAY 1 - 3
Locate Records – make sure you check both electronic and manual records. Do we have any records which would satisfy the request? You must take all reasonable action to locate all records



DAY 4 - 7
Once the likely locations of the requested data have been identified, it should all be collated in order to review it and determine what can be disclosed.



DAY 7-15
Do any exemptions apply to the records? Depending on the reason for the request not everything in the records will need to be disclosed?



DAY 7-15
Is third party information contained in the records? Does the requester have authority to view this? If NO, this needs to be clearly anonymised



DAY 7-15
When anonymising information it need to be done so it is obvious information has been removed. The best way to do this is with a black marker or where the documents are electronic use the black colour highlight tool



DAY 15-20
Copy all the relevant records which are to be disclosed. Make sure the information which has been redacted remains unreadable and obvious that information has been removed



DAY 20-25
Prepare a schedule of documents which satisfy the request and which are to be disclosed. Make sure you identify where redactions have been made and why.



DAY 25-28
If appropriate, include a list of definitions or explanations where the records contain particularly complex or technical terminology



DAY 25-28
Once satisfied they records are appropriate to be disclosed and the schedule is a complete log, records must be checked by nomintaed officer



Day 28-30
Arrange to appropriately disclose the records to the third party – will this be done face to face? Electronically? However this is done must be secure!



Day 30
Once disclosure complete, notify the service and update the log

2. INTRODUCTION

- 2.1 The Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) gives individuals the right of access to personal information held about them by an organisation. This right is set out in Article 15 of the EU General Data Protection Regulations (GDPR) and such a request is known as a 'subject access request' (SAR). The rights of subject access constitute a statutory duty and must be treated as a priority.
- 2.2 Failure to respond to a SAR within the legal timeframe may result in enforcement action brought by the Information Commissioner's Office (ICO) which is responsible for enforcing the DPA. It is imperative that all SARs are dealt with promptly. If you are unclear about your obligations, please seek advice as soon as possible. Details of who to contact for advice and assistance can be found at Part 10 of this Guidance.

3. SCOPE OF THIS GUIDANCE

- 3.1 This guidance has been drawn up to assist employees in understanding how to recognise and respond to a SAR in compliance with the Council's obligations under the DPA. It explains the right of access to personal data and the procedures that must be followed. A failure to follow this guidance may result in **disciplinary action**.
- 3.2 This guidance applies to all employees, including those who may respond to a SAR. It also applies to all personal information whether manual, electronic, audio or visual. This guidance should be read in conjunction with the Council's other related documents which include:
- [Information Governance Framework – Conduct Policy](#)
 - [Subject Access Requests - A basic guide to Redaction](#)
 - Pro-forma letters
- These documents and other useful information can be found on the Council's [Information Governance Intranet page](#).

4. THE RIGHT OF SUBJECT ACCESS

- 4.1 Individuals data rights are set out in the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) Almost all of these rights are subject to limitations and exceptions. The main right is that of subject access but there are others. The right of subject access includes access to *personal data*:
- processed electronically on a computer;
 - Accessible records (for example housing tenancy files, social work files);
 - Manual records held in a *relevant filing system*;
 - In respect of public authorities subject to the Freedom of Information Act 2000 (FOIA) only, access to *unstructured* manual records which are not held in a *relevant filing system*.
- 4.2 The right of subject access allows a living individual ("the data subject") to find out what information ("personal data") is held by an organisation about them. Upon receipt of a valid SAR, the Council is required to provide the following information to the requester:
- Confirmation as to whether any personal data is being processed;
 - A description of the personal data, the reasons it is being processed and whether it has/will be given to other organisations/people;
 - A copy of the personal data (which may be copies of the original documents or a transcript which is specially prepared in order to respond to the SAR); and
 - Details as to the source of the data (where this is available).

- 4.3 Information must be provided in a permanent format (e.g. by supplying copies of records where appropriate) and all information must be legible. Any acronyms or jargon should be explained to the data subject in the response. If a data subject only requires a copy of their personal data then you are not required to provide the other information listed above under (a), (b) and (d).
- 4.4 Further guidance on identifying personal information can be found at **Appendix 1**.
- 4.5 Under the General Data Protection Regulations the rights for individuals have been enhanced and further guidance is available on the Information Commissioner's Office website <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights>. The following rights are now provided:-
- The right to be informed
 - The right of access
 - The right to rectification
 - The right to erasure
 - The right to restrict processing
 - The right to data portability
 - The right to object
 - Rights in relation to automated decision making and profiling.

5. ROLES AND RESPONSIBILITIES

- 5.1 Most SAR requests are sent directly to **Executive Support**, who will log the request and assign it to the appropriate officer within the relevant Directorate to deal with. Where a request is received by a service area directly, they will be responsible for ensuring that the request is logged within 24 hours of receiving it by sending a copy of the request by email to **Executive Support** (executivesupport@tameside.gov.uk)
- 5.2 All officers are responsible for recognising a SAR and following the appropriate steps to progress it, whether this means gathering the information requested personally, or transferring it to the appropriate person to deal with.
- 5.3 All managers/team leaders are responsible for being aware of the SAR procedure and cascading it to their team members. They are also responsible (where nominated by the Head of Service) for approving the response, notifying the **Directorate IG Champions** with issues and seeking advice and assistance where needed.
- 5.4 **Heads of Service**
Heads of Service are assigned responsibility for the main systems and information assets within their business area. The Head of Service is responsible for monitoring compliance with the DPA in respect of the information they 'own', which includes compliance with the right of subject access. They are responsible for selecting appropriate officers within their Service to be responsible for dealing with SARs and identifying different senior officers within their Service to act as Directorate IG Champions. In the event of a complaint about the way a SAR has been handled, the Head of Service is responsible ensuring the complaint is properly investigated and approving the response.
- 5.5 **Directorate IG Champions**
Directorate IG Champions have been appointed within Directorates to provide advice and support for officers who have been assigned a SAR to respond to. The Directorate IG Champions will also review information prior to disclosure following a SAR to ensure that the correct information is being disclosed and/or all appropriate redactions have been made.

In most cases an IG Champion will be a Service Unit Managers as they have an understanding of the service area and the information governance issues involved. They are also normally responsible for data protection or freedom of information as part of their job role.

All Directorate IG Champions will receive training in the handling of SARs and will therefore have a greater level of expertise than most officers in handling a SAR.

5.6 Further Advice and Assistance

There will be occasions where further advice and assistance is required.

- Process queries, should be directed to Executive Support (0161 342 3017)
- Disclosure/redaction queries should be directed in the first instance to the Risk and Insurance Team (0161 342 3859).
- Information Champions

6. WHAT MAKES A VALID SAR REQUEST?

6.1 Time limit for complying with a SAR

All SARs should be responded to promptly, and in most cases the maximum time limit for responding to a SAR is 1 calendar month once the following has been received by the Council:

- The written request;
- Clarification from the requester (where requested);
- Satisfactory proof of identity (where requested); and

6.2 Request to be in writing

A valid SAR must be made in writing, but it does not need to refer to legislation or mention the phrase “subject access”. Even if the request refers to other legislation, such as the Freedom of Information Act, if it is a request for personal information of the person making the request (the data subject) it should be treated as a SAR. If the request refers to the Freedom of Information Act you will need to send a refusal notice relying on s40 (1) of the FOIA – see the attached link: - <http://intranet2.tameside.gov.uk/corpserv/solicitor/proformadocs.doc> .

6.3 Any written request which makes clear that personal information is being requested should be handled as a SAR and logged in accordance with the process set out in section four above.

6.4 The Council has a duty to make reasonable adjustments in the case of individuals who are disabled, so it may be appropriate as a reasonable adjustment to act upon a verbal request for information and handle it as a SAR. In such a case, the oral request should be documented in an accessible format and provided to the applicant or their advocate (if authorised) in writing so that both parties are clear about how the request is being handled.

6.5 In some cases, a request for personal data may be handled in the normal course of business, for example, if a customer asks for a further copy of information that they have misplaced. Such a request does not have to be dealt with formally as a SAR so long as it is dealt with promptly, and in any event, **within 1 calendar month**.

6.6 Some SARs may reach the Council through a third party that is processing personal data on the Council’s behalf (“a data processor”). All SARs notified to the Council by a data processor must be dealt with as set out in this Guidance. In addition, receipt of a SAR from a data processor must be acknowledged in writing and clear instructions given as to any further information or action required from the data processor in dealing with the SAR.

6.7 **Asking for clarification**

If the wording of the request does not clearly identify the information that the requester is seeking, a letter must be sent to them promptly (and in any event within 3 working days) which asks them to provide further clarification to assist in locating the required information.

This might include asking the requester to identify particular departments, names of officers or specific dates etc., in relation to the information that they require. Whilst clarification can be sought, the requester must not be asked to narrow the scope of their request. If a requester has asked for “all information you hold about me”, they are entitled to do so.

6.8 **Proof of identity**

It is important that the identity of the requester is verified to avoid information about one individual being sent to somebody else, either in error or as a result of deception. If the requestor is unknown to the employee processing the request, a letter must be sent to the requestor promptly (and in any event within 3 working days) asking them to provide two forms of identification, one of which should include their current address. If, following the provision of these documents, the employee processing the SAR is not satisfied about the identity of the requestor, they should contact the Directorate IG Champion.

Part 6 of this guidance explains what to do if a SAR is made by a third party on behalf of another person

6.10 **Requests made on behalf of others**

The DPA does not prevent an individual from giving permission to a third party to make a SAR on their behalf. For example, a data subject may instruct a solicitor, friend or family member to make a SAR on their behalf. It is up to the third party to provide satisfactory proof that they have been given authority to make the request. Documentary proof of this, such as a letter of authority signed by the data subject or a power of attorney, must be provided by the requestor. If there is any doubt about the authority given to the third party, information must not be disclosed and advice should be sought from the Directorate IG Champion.

7. **REQUESTS FOR INFORMATION ABOUT CHILDREN**

7.1 It is important to remember that personal data about a child, however young, is the child’s personal data and is not the personal data of their parent or guardian. The age of consent for children is 13 as prescribed by Article 8 of the EU General Data Protection Regulations (GDPR).

7.2 A parent or guardian does not have an automatic right to personal data about their child and can only apply on the child’s behalf if the child:

- has given consent; or
- is too young to have an understanding to make the application.

7.3 There is no fixed age at which a child may exercise their rights under the DPA, including the right of subject access. Any age may be appropriate if the young person has sufficient maturity/capacity. Children can make a subject access request if they are capable of understanding the nature of the request.

8. **HANDLING THE SAR**

8.1 Once a complete SAR is received, the 1 calendar month in which the SAR must be completed will commence. In the interest of good customer service, where possible we should aim to provide the requested information as soon as is practical. A [SAR Checklist](#)

should be completed at all stages. The flowchart at the beginning of this document gives guidance on the handling of a SAR.

8.2 In order for the Council to meet the statutory timescale the following timescales should be followed:-

- **Locating the requested information – Days 1-3**

The location of all recorded data on the data subject, whether it is electronic or stored in paper files, must be identified within 3 days of receipt of the complete SAR. In many cases this will involve searching any electronic system used within your business area (e.g. ICS / IAS) and may also include a search of emails.

Where it is identified that information is likely to be stored in email accounts, appropriate approval must be sought the process outlined in the ICT Security Access Procedure must be followed. A reasonable effort must be made to identify if any relevant information may be held within other service areas which should be disclosed as part of the SAR.

- **Collating the requested information - Days 4-7**

Once the likely locations of the requested data have been identified, it should all be collated in order to review it and determine what can be disclosed.

- **Reviewing the information, deciding what to disclose, making the redactions and drafting the response letter – Days 7-15**

The information must be carefully reviewed to determine whether some of it may be exempt from disclosure. **Further advice about whether an exemption applies may be required, so it is important that this process begins as soon as possible.** Further assistance is available in the guidance document "[Subject Access Requests - A basic guide to Redaction](#)"

If there is information to be redacted (this means the removal of information from a document that should not be disclosed to the requester) the following process should be used:-

- Information to be redacted should be approved by the Directorate IG Champion before the source material is copied.
- Once approved, the source material should be copied on single sided A4 paper and any redactions carried out manually using a black marker or electronically using Adobe Acrobat or bespoke redaction software.
- The Quality Assurance step detailed below must be followed before any information is disclosed to the requestor.

If information is withheld in reliance on an exemption, the requestor is entitled to receive an explanation in plain English detailing the fact that information has been withheld and the reasons why. The explanation must be more than simply specify that a particular exemption applies.

- **Quality Assurance – Days 25-28**

In any case where it is proposed that an exemption should apply in order to withhold or redact information, this must be reviewed by an appropriate other person. This will normally be the Directorate IG Champion. The proposed response letter and information should be referred to the Directorate IG Champion together with the IG Checklist.

The Directorate IG Champion will then be required to review the proposed response and information to check that the use of exemptions is appropriate. The Directorate IG Champion must complete the Quality Assurance section of the SAR Checklist.

This should then be referred back to the officer handling the SAR, who will be responsible for making the final disclosure.

- **Making the disclosure – Days 28-30**

Every effort should be made to ensure that the response letter is addressed to the correct person, has the correct address and the information being disclosed is about the right person. The response must be sent by a suitably secure method, and evidence of this must be retained. For example, if being sent by post, the response should be sent by Royal Mail Signed for Delivery, and where the response is sent by email, the content should be sent using Egress Switch.

All documents disclosed to the requester must be listed on a document schedule (**Appendix 2**) which will include details of the justification behind information being redacted. Copies of the documents that have been disclosed to the requester must be marked with “**Redacted documents disclosed to the Data Subject**” and retained. A complete copy of the un-redacted documents must also be retained.

- **Delays**

If there will be a delay in providing a complete response to the SAR, for example because of the volume of information or the complexity in redacting the information, the officer handling the SAR must notify **Executive Support who can then inform the requestor**. As much information as possible should be given within the 40 day time limit and only delay responding where this is unavoidable. This is important to ensure good customer service and to provide as evidence to the Information Commissioner (where appropriate) in respect of a complaint about any delay in responding to a SAR.

Failure to comply with the 40 days allowed to respond to a SAR may leave the Council open to not only reputational damage and the scrutiny of the Information Commissioner but also potential enforcement action and fines. Where staff fail to comply with this statutory duty under the Data Protection Act disciplinary action may be taken.

8.3 **Format of information**

In order to comply with a SAR, in many cases it will be convenient to supply the requester with copies of documents (redacted where appropriate). However, the right of subject access under the DPA is not a right to copies of documents. In some cases, SAR compliance may be achieved by producing a transcript of the personal data and supplying this to the requester, rather than providing heavily redacted documents. Must be in a clear, easily accessible format, where possible electronic

9. **REQUESTS INVOLVING THIRD PARTY PERSONAL DATA**

9.1 The Council does not have to comply with a SAR to the extent that it would mean disclosing information about another individual who can be identified from that information, except where either:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

9.2 In many cases the requested information will include the personal data of the requester and will also identify other people. Where information relates to the data subject and also includes information about another individual, an assessment will need to be made as to whether information identifying another person should be disclosed. For the avoidance of

doubt, information that solely relates to the data subject who has submitted the SAR must be disclosed (unless it is otherwise exempt).

- 9.3 The ICO has issued a [Subject Access Code of Practice](#) which provides guidance on the handling of SARs. It suggests three steps when handling SARs involving other people's information. These are summarised below.

- **Step One: Does the request require the disclosure of information that identifies a third party?**

The ICO suggest that when considering whether it is possible to comply with the request without providing information that identifies other individuals, you should take into account any information that you disclose and also any information you reasonably believe that the requester may have, or may get hold of, that would identify the third party(ies).

If it is possible to do so, then names/information about third parties can be redacted or withheld when making the disclosure. If it is not possible to separate the third-party information from the personal data of the data subject making the SAR, then Steps Two and Three should be considered.

- **Step Two: Has the third-party individual consented?**

If it is appropriate to seek consent, and the third party does consent, the information can be disclosed. There is no obligation under the DPA to seek consent, and sometimes this will not be possible, for example in relation to old social work records when the whereabouts of individuals will be unknown.

In some cases it may not be appropriate to seek the consent of the third party; for example, where the third party is a perpetrator/alleged perpetrator of abuse against the data subject, it may be ill-advised to approach the third party especially as this will inevitably involve a disclosure to them about the SAR that has been made. If it is not appropriate or possible to seek consent, or where consent has been refused, then Step Three should be considered.

- **Step Three: Would it be reasonable in all the circumstances to disclose without consent?**

An assessment as to whether it would be reasonable in all the circumstances to make the disclosure will need to be undertaken. This assessment would be best undertaken by, or in consultation with, an officer who has been involved in dealing with the data subject or is at least aware of the circumstances of the case. In cases where the information is not recent, it is accepted that this will not be possible and therefore the assessment of what is reasonable will need to be undertaken by an officer having read the paperwork.

- 9.4 The DPA itself suggests various factors which ought to be considered when deciding whether it is reasonable to disclose information where a third party would be identified. These factors are:

- Any duty of confidentiality owed to the third party;
- Any steps taken to try to obtain the consent of the third party;
- Whether the third party is capable of giving consent;
- Express refusal of consent of the third party.

9.5 **Duty of confidence owed to a third party**

A duty of confidence can arise where information has the necessary quality of confidence (which means that it is not generally available to the public and is not trivial) and is imparted in circumstances whereby the party making the disclosure has a reasonable expectation that the information will remain confidential. Some relationships carry a general duty of

confidence e.g. doctor/patient, solicitor/client. As a general rule, where a duty of confidence is owed to a third party, it would not be reasonable to disclose such information. Advice should be sought if the employee dealing with the SAR is unsure.

9.6 **Other relevant factors**

The ICO's guidance also suggests other relevant factors that may be considered: "Information generally known by the individual making the request. If the third party information has previously been provided to the individual making the request, is already known to them, or is generally available to the public, it will be more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual."

9.7 **Circumstances relating to the individual making the request**

The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent."

9.8 **Information about Council officers**

As a general presumption, information identifying Council officers acting in their professional capacity may be disclosed. However, this should be considered on a case by case basis according to the principles outlined above. Advice should be sought if the employee dealing with the SAR is unsure.

There are special rules about the disclosure of third party data where the third parties are professionals in health, education or social work. In general terms, such information does not need to be redacted unless disclosure of the officer's identity would put their health and safety at risk. Advice should be sought if the employee dealing with the SAR is unsure.

10. **EXEMPTIONS**

10.1 In some cases exemptions may be applied, which means that certain information may not need to be disclosed to the data subject in response to their SAR. The DPA includes a number of exemptions but this Guidance only explains those which are most relevant to the information held by the Council. If there are still concerns about disclosing information, then advice should be sought from your Directorate IG Champion.

10.2 **Third Party Information**

As a general rule, information about third parties should not be disclosed without that person's consent. There will be times when it would not be possible or appropriate to seek consent of the third party, so you will then need to consider whether it is reasonable to disclose information that identifies a third party. For example, it may be reasonable to release names of third parties without seeking express consent, i.e. where it is clear that the enquirer already knows the information about the third party.

10.3 **Crime and taxation**

Information can be exempt if the disclosure of that information in response to the SAR would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the collection of any tax or duty. For example, this might apply to information about an individual that has been shared with the Police in respect of an ongoing investigation. It might also apply to information about an individual who is being investigated for council tax fraud.

If this exemption does apply to information, care must be taken when responding to the SAR. In some cases, the response may “tip off” an individual by explaining the reasons why information is being withheld under this exemption. It is therefore suggested that advice is sought where this exemption applies.

10.4 **Health, social work and education**

Some information relating to health, social work and education may be exempt from disclosure in certain circumstances. If the documents include medical information, which came from a health professional, the general rule is that a health professional must be consulted to establish whether disclosing the information could be detrimental to the individual concerned. There are exceptions to this so advice must be sought where there is doubt about whether consultation with a health professional is required.

If the documents include health data about the requester (other than information which was provided by a health professional) and it is considered that disclosure may cause serious harm to the physical or mental health of the individual or any other person, advice should be sought as there may be requirement to consult with a health professional before any disclosure is made.

Special rules apply where releasing information about social services and related activities that could impact on delivery of social work by causing serious harm to the physical or mental health of the individual or any other person. Any such information must be redacted. Occasions where this exemption applies are few but if it may apply, the relevant and involved Social Worker must be consulted and advice sought from the Directorate IG Champion. Data should not be withheld simply because the individual is likely to make a complaint about a social worker when they see the information.

10.5 **Confidential references**

A reference provided by the Council about the data subject to another party is exempt from disclosure. A reference received by the Council from another party will not be caught by this exemption.

10.6 **Publicly available information**

Any personal data that the Council is required to publish is exempt.

10.7 **Negotiations with the requester**

This exemption may apply to information about the Council’s intentions in negotiations with an individual to the extent that complying with a SAR would be likely to prejudice the negotiations. For example, this exemption might apply in relation to negotiations relating to Employment Tribunal proceedings.

10.8 **Legal professional privilege**

Where legal advice has been sought or where there are or have been legal proceedings, information may be covered by legal professional privilege and may be exempt from disclosure. **Legal Services should always be consulted in these cases before making any disclosure.**

11. **COMPLAINTS ABOUT SUBJECT ACCESS**

- 11.1 Where a requester is not satisfied with the response to their SAR, the Council offers an internal review. Where a complaint is received, a senior manager (who will not be the officer who made the original decision) must immediately notify Sandra Stewart as the Data Protection Officer. The senior manager must then investigate the complaint and report to Sandra Stewart within 5 working days on the outcome of the investigation.

- 11.2 In addition to the internal review process, a data subject may also refer their complaint to the ICO, or may take action through the courts to enforce their right of subject access.
- 11.2 A separate protocol is in place for dealing with requests from the Police and the Crown Prosecution Services (CPS) and the Single Point of Contact (SPoC) is Danielle Cunningham-Hobbs (Risk, Insurance and Information Officer) within the Risk Management and Audit Service.

Q1 - Can a living person be identified from the information or in conjunction with that and other information held by the Council?

- Yes - Proceed to Q2
- No - Not personal data
- Unsure - Proceed to Q2

Q2 - Does the information relate to an individual (in a personal or professional sense)?

- Yes - It is likely to be personal data
- No - Not personal data
- Unsure - Proceed to Q3

Q3 - Is the information 'obviously about' a particular individual?

- Yes - It is personal data
- No - Proceed to Q4
- Unsure - Proceed to Q4

Q4 - Is the information 'linked to' an individual so that it provides particular information about an individual?

- Yes - It is personal data
- No - Proceed to Q5
- Unsure- Proceed to Q5

Q5 - Is the information used, or will it be used, to inform/influence actions or decisions affecting an identifiable person?

- Yes - It is personal data
- No - Proceed to Q6
- Unsure - Proceed to Q6

Q6 - Does the information have any biographical significance to the individual?

- Yes - It is likely to be personal data
- No - Proceed to Q7
- Unsure - Proceed to Q7

Q7 - Does the information focus/concentrate on the individual as its central theme, rather than another individual, object, transaction or event?

- Yes - It is likely to be personal data
- No - Proceed to Q8
- Unsure - Proceed to Q8

Q8 - Does the information impact or have the potential to impact on the individual, in personal, family, business or professional capacity?

- Yes - It is likely to be personal data
- No
- Unsure - Seek advice from Legal Services or Risk Management

SCHEDULE OF DISCLOSED DOCUMENTS**APPENDIX 2**

SCHEDULE OF DOCUMENTS DISCLOSED IN RESPONSE TO SUBJECT ACCESS REQUEST		
Ref	Page No.	Details (including redaction rationale)
1	If only providing part of a report list which page number i.e. 8-10	Example....Psychological report of parent dated 01/01/2010 As the information relates mainly to the parent and their relationships/health etc. the report has been redacted to protect the third parties information as this is either unknown to the requester or protected information.
2		
3		
4		

This page is intentionally left blank

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officers:	Kathy Roe – Director of Finance Paddy Dowdall - Assistant Director of Pensions (Local Investments and Property)
Subject:	GMPF STATEMENT OF ACCOUNTS 2017-2018 GOVERNANCE ARRANGEMENTS
Report Summary:	This report aims to inform the Panel of the governance arrangements for approval of the accounts for Greater Manchester Pension Fund (GMPF) as part of the accounts of Tameside MBC as administering authority. Secondly, the report asks Members to note the key assumptions for estimates used in the GMPF accounts
Recommendations:	<ul style="list-style-type: none">(i) To note the governance arrangements for approval of GMPF accounts.(ii) To note the assumptions for estimates used in the GMPF accounts.
Financial Implications: (Authorised by the Section 151 Officer)	<p>As the administering authority, Tameside MBC has important responsibilities in relation to the Greater Manchester Pension Fund. However, as the largest fund in the Local Government Pension Scheme, GMPF also has significant resources it deploys to meet those responsibilities. This paper sets out where the responsibilities lie.</p> <p>The assumptions used for valuing assets will have an impact on the value of assets reported in the accounts. In most circumstances the impact is unlikely to be material. For equities and bonds a bid basis is used that results in a more prudent outcome (v mid or offer basis).</p>
Legal Implications: (Authorised by the Solicitor to the Fund)	The administering authority must produce an annual report and accounts.
Risk Management:	GMPF's accounts are used to provide information to a variety of users and for a variety of purposes. The accuracy of the statements is critical in the determination of employer costs and there are clearly reputational issues relating to the validity of the accounts. The audit process provides reassurance on the integrity of the statements and mitigates against the possibility of material misstatement
ACCESS TO INFORMATION:	NON-CONFIDENTIAL This report does not contain information which warrants its consideration in the absence of the Press or members of the public.

Background Papers:

Any enquiries should be directed to Tracey Boyle, 0161-301-7116 (email: tracey.boyle@tameside.gov.uk)

1. INTRODUCTION

1.1 This report covers two sections:

- Governance Arrangements for the approval of the accounts;
- Noting of the on-going key assumptions made in compiling the accounts: and

1.2 The governance arrangements for approval of the accounts are consistent with last year, when they were brought forward as a consequence of changes for the statutory deadlines for local authorities to produce their accounts which became mandatory in 2018.

2. GOVERNANCE ARRANGEMENTS

2.1 The Management Panel approves the GMPF accounts and formal letters required by the external auditor. It also receives external audit reports.

2.2 The key decision making bodies for the Council are the Audit Panel which receives accounting policies reports for both GMPF and the Council and the Overview (Audit) Panel which receives the report of the external auditor following the audit of the accounts. The Council retains overall responsibility for the accounts of both, and the follow-up on the audit reports received for both, but in practice delegates the responsibility for GMPF to GMPF.

2.3 The provisional timetable for approval of the accounts and audit reports by these bodies for 2017/18 is outlined in the table below.

Date	Group	Stage
20 April 2018	Employer Funding Working Group	Noting of continued key assumptions and updated governance arrangements (GMPF)
TBC (provisionally 29 May 2018)	Audit Panel	Approval of key assumptions and noting of governance arrangements (TMBC and GMPF)
TBC (provisionally 20 July 2018)	GMPF Management Panel	Approval of final accounts, annual report and audit report (GMPF)
TBC (By 31 July 2017)	Overview (Audit) Panel	Approval of final accounts, annual report and audit report (GMPF and TMBC)

2.4 The plan this year, due to the legal requirement from 2017/18, is that the pre-audit accounts of both TMBC and GMPF are signed off by the S151 officer of the Council by 31 May 2018.

2.5 The review by the external auditors commences thereafter. Grant Thornton LLP provide the external audit contract for both, but a separate team conduct the GMPF audit due to the specialist and technical demands of LGPS accounts.

2.6 To comply with the statutory arrangements from 2017/18 onwards, the process will be completed by 31 July 2018.

3. CONTINUED KEY ASSUMPTIONS

3.1 The key continuing assumptions used in production of the accounts will be disclosed in note 2 of the GMPF accounts when produced:

- Accruals basis
- Fair value for investments
- Market prices at bid where possible
- For non-listed assets, compliance with accounting standards and best practice

- Liabilities in compliance with International Accounting Standard 19 (IAS19)
- Continued phased implementation of CIPFA's guidance on accounting for management costs in the LGPS

4. RECOMMENDATION

- 4.1 To note the governance arrangements for the approval of GMPF's accounts.
- 4.2 To note the continued assumptions for estimates to be used in the GMPF Statement of Accounts.

Report To:	AUDIT PANEL
Date:	29 May 2018
Reporting Officers:	Kathy Roe – Director of Finance Paddy Dowdall - Assistant Director of Pensions (Local Investments and Property)
Subject:	GMPF EXTERNAL AUDIT PLAN 2017-18
Report Summary:	<p>As GMPF's appointed External Auditors for 2017-18, Grant Thornton are required to undertake work to enable them to form and express an opinion on the financial statements that have been prepared by management with the oversight of those charged with governance.</p> <p>The audit plan provides an overview of the planned scope and timing of the statutory audit of GMPF.</p>
Recommendations:	That the external plan for 2017-18 is noted.
Links to Community Strategy:	Effective corporate governance and a robust approach to economy, efficiency and effectiveness underpin the delivery of the Community Strategy.
Policy Implications:	There are no wider policy implications arising from this report.
Financial Implications: (Authorised by the Section 151 Officer)	There are no direct financial implications arising from this report.
Legal Implications: (Authorised by the Borough Solicitor)	Demonstrates the Council's compliance with the Accounts and Audit Regulations 2011.
Risk Management:	The Council has arrangements in place to ensure that the Council meets the required standards in financial reporting, and that robust arrangements are in place to ensure economy, efficiency and effectiveness in the use of resources. External Audit provides a source of assurance over these arrangements.
Access to Information:	<p>The background papers relating to this report and any further information can be obtained from the report writer, Tracey Boyle, Head of Pensions Accountancy.</p> <p>Telephone: 0161 342 2929</p> <p>e-mail: tracey.boyle@tameside.gov.uk</p>

This page is intentionally left blank

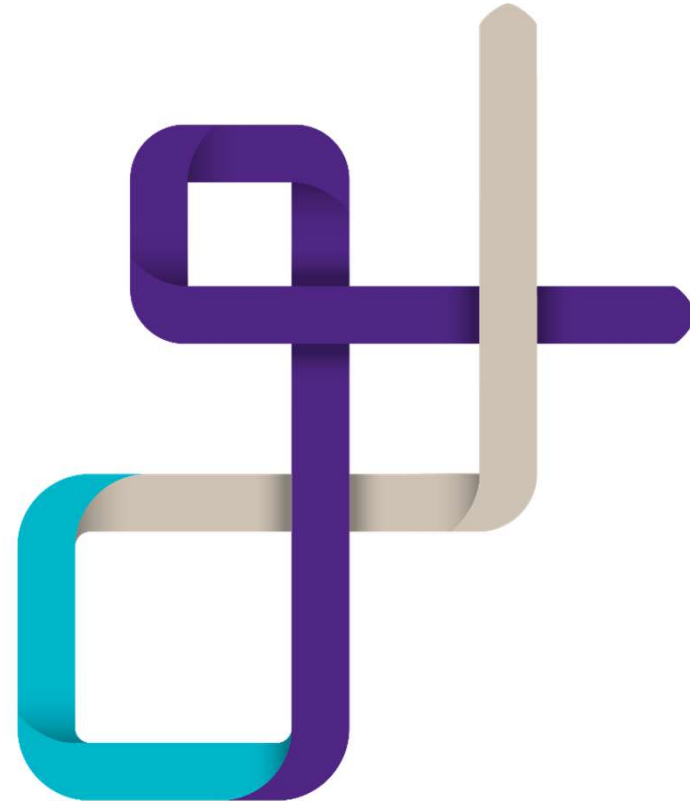
External Audit Plan

Year ending 31 March 2018

Greater Manchester Pension Fund

9 March 2018

Page 239



Contents



Your key Grant Thornton team members are:

Page 240

Mike Thomas
Director

T: 0161 214 6368
E: mike.thomas@uk.gt.com

Marianne Dixon
Manager

T: 0113 200 2699
E: marianne.dixon@uk.gt.com

Mark Stansfield
Executive – In charge

T: 0161 234 6356
E: mark.stansfield@uk.gt.com

Section	Page
1. Introduction & headlines	3
2. Deep business understanding	4
3. Significant risks identified	5
4. Reasonably possible risks identified	7
5. Other matters	9
6. Materiality	10
7. Audit logistics, team & audit fees	11
8. Early close	12
9. Independence & non-audit services	13
Appendices	
A. Revised ISAs	14

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit planning process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect the Fund or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Grant Thornton UK LLP is a limited liability partnership registered in England and Wales: No.OC307742. Registered office: 30 Finsbury Square, London, EC2A 1AG. A list of members is available from our registered office. Grant Thornton UK LLP is authorised and regulated by the Financial Conduct Authority. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

Introduction & headlines

Purpose

This document provides an overview of the planned scope and timing of the statutory audit of Greater Manchester Pension Fund ('the Fund') for those charged with governance.

Respective responsibilities

The National Audit Office ('the NAO') has issued a document entitled Code of Audit Practice ('the Code'). This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. Our respective responsibilities are also set in the Terms of Appointment and Statement of Responsibilities issued by Public Sector Audit Appointments (PSAA), the body responsible for appointing us as auditor of Greater Manchester Pension Fund]. We draw your attention to both of these documents on the [PSAA website](#).

Scope of our audit

The scope of our audit is set in accordance with the Code and International Standards on Auditing (ISAs) (UK). We are responsible for forming and expressing an opinion on the financial statements that have been prepared by management with the oversight of those charged with governance the Overview (Audit) Panel of Tameside MBC.

The audit of the financial statements does not relieve management or the Overview (Audit) Panel of your responsibilities.

Our audit approach is based on a thorough understanding of the Fund's business and is risk based.

Significant risks

Those risks requiring specific audit consideration and procedures to address the likelihood of a material financial statement error have been identified as:

- Fraud in revenue recognition – This risk has been rebutted for the Fund as documented on page 5
- Management over-ride of controls
- Valuation of Level 3 Investments.

We will communicate significant findings on these areas as well as any other significant matters arising from the audit to you in our Audit Findings (ISA 260) Report.

Materiality

We have determined planning materiality to be £212.7m (PY £212.7m), which equates to 1% of your net assets. We are obliged to report uncorrected omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. Clearly trivial has been set at £10.6m (PY £10.6m).

Audit logistics

Our interim visit will take place in March 2018 and our final visit will take place in June 2018. Our key deliverables are this Audit Plan and our Audit Findings Report.

Our fee for the audit will be no less than £56,341 (PY: £56,341) for the Fund. Where requests are received from other auditors of other bodies for assurance in respect of information held by the Fund and provided to the actuary to support their individual IAS 19 calculations these will be billed in addition to the audit fee on a case by case basis. We estimate this fee to be £5,996 for 2017-18.

Independence

We have complied with the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements

Deep business understanding

Changes to service delivery

Pooling

Arrangements for the pooling of investments continue to develop. The DCLG have reported on the progress of pools and noted the pace of development, including the launching of procurements for pool operators, appointing senior officers and preparing applications for Financial Conduct Authority authorisation. This remains a challenging agenda, with arrangements required to be in place from 1 April 2018. These arrangements will have a significant impact on how investments are managed and monitored, with much of the operational responsibility moving to the pool operator. It remains key that administering authorities (through Pension Committees and Pension Boards) continue to operate strong governance arrangements, particularly during the transition phase where funds are likely to have a mix of investment management arrangements. We will continue to discuss with fund officers their plans for asset pooling and the implications this will have on the investment policy and governance arrangements of the fund.

Markets in Financial Instrument Directive (MiFID II)

January 2018 saw the implementation of MiFID II. The impact for the Fund is that to be able to continue to access the same investments as previously, it needed to apply to 'opt up' and gain election to professional status. Without this change in status some financial institutions could terminate their relationship with the Fund, which may have an adverse impact on the achievement of the investment strategy.

On-going Matters

- Indexation and equalisation of GMP in public service pensions schemes
- Reforms to public sector exit packages and the application, or not, of the 2013 Fair Deal changes to the LGPS
- SAB work on options for academies within the LGPS and review of Tier 3 employer risks

Changes to financial reporting requirements

Accounts and Audit Regulations 2015 (the Regulations)

The Department of Communities and Local Government (DCLG) is currently undertaking a review of the Regulations, which may be subject to change. The date for any proposed changes has yet to be confirmed, so it is not yet clear or whether they will apply to the 2017/18 financial statements.

Under the 2015 Regulations local authorities are required to publish their accounts along with the auditors opinion by 31 July 2018.

Changes to the CIPFA 2017/18 Accounting Code

CIPFA have introduced minor changes to the 2017/18 Code, these include a new disclosure of investment manager transaction costs and clarification on the approach to investment concentration disclosure.

Key challenges

Financial pressures

At the latest triennial valuation (31 March 2016) the fund had sufficient assets to cover 95% of liabilities. This was an improvement from 93% as at 31 March 2013. The Fund's assets are now valued at over £21bn. The Fund has a strong approach to governance which has delivered strong financial performance over many years despite exceptionally low long term interest rates. It continues to achieve investment performance in excess of benchmark; stable contribution rates for employers whilst continuing to develop local investment opportunities.

General Data Protection Regulations (GDPR)

GDPR comes into effect in May 2018 and replaces the Data Protection Act 1998. It introduces new obligations on data controllers. The Fund is both a data controller and a data processor and needs to ensure that it has appropriate processes in place to comply with the changes being introduced.

tPR 2016 Governance and Administration Survey

Published in May 2017 whilst showing improvements in governance tPR noted that its focus for 2017/18 would be scheme governance, record keeping, internal controls and member communication and that tolerance for scheme shortcomings in these areas was reducing and that they were more likely to use their enforcement powers where scheme managers have not taken sufficient action to address issues or meet their duties.

Our response

- We will consider whether your financial position leads to uncertainty about the going concern assumption and will review any related disclosures in the financial statements.
- We will keep you informed of changes to the Regulations and any associated changes to financial reporting or public inspection requirements for 2017/18 through on-going discussions.
- As part of our opinion on your financial statements, we will consider whether your financial statements reflect the financial reporting changes in the 2017/18 CIPFA Code.

Significant risks identified

Significant risks are defined by professional standards as risks that, in the judgement of the auditor, require special audit consideration because they have a higher risk of material misstatement. Such risks often relate to significant non-routine transactions and judgmental matters. In identifying risks, audit teams consider the nature of the risk, the potential magnitude of misstatement, and its likelihood.

Risk	Reason for risk identification	Key aspects of our proposed response to the risk
The revenue cycle includes fraudulent transactions	<p>Under ISA (UK) 240 there is a rebuttable presumed risk that revenue may be misstated due to the improper recognition of revenue. This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.</p>	<p>Having considered the risk factors set out in ISA240 and the nature of the revenue streams at the Fund, we have determined that the risk of fraud arising from revenue recognition can be rebutted, because:</p> <ul style="list-style-type: none">• there is little incentive to manipulate revenue recognition• opportunities to manipulate revenue recognition are very limited• the culture and ethical frameworks of local authorities, including Tameside Metropolitan Borough Council as the Administering Authority of Greater Manchester Pension Fund, mean that all forms of fraud are seen as unacceptable <p>Therefore we do not consider this to be a significant risk for Greater Manchester Pension</p>
Management over-ride of controls	<p>Under ISA (UK) 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities. Management over-ride of controls is a risk requiring special audit consideration.</p>	<p>We will:</p> <ul style="list-style-type: none">• gain an understanding of the accounting estimates, judgements applied and decisions made by management and consider their reasonableness• obtain a full listing of journal entries, identify and test unusual journal entries for appropriateness• evaluate the rationale for any changes in accounting policies or significant unusual transactions.

Significant risks identified

Risk	Reason for risk identification	Key aspects of our proposed response to the risk
The valuation of Level 3 investments is incorrect	Under ISA 315 significant risks often relate to significant non-routine transactions and judgemental matters. Level 3 investments by their very nature require a significant degree of judgement to reach an appropriate valuation at year end.	<p>We will:.</p> <ul style="list-style-type: none"> review the nature and basis of estimated values and consider what assurance management has over the year end valuations provided for these types of investments. consider the competence, expertise and objectivity of any management experts used. Review the qualifications of the fund managers as experts to value the level 3 investments at year end and gain an understanding of how the valuation of these investments has been reached. For indirect property investments, test valuations to valuation reports and/or other supporting documentation. For a sample of private equity investments, test valuations to fund manager valuations and/or by obtaining and reviewing the audited accounts at latest date for individual investments and agreeing these to the fund manager reports at that date. Reconciliation of those values to the values at 31st March with reference to known movements in the intervening period.

Reasonably possible risks identified

Reasonably possible risks (RPRs) are, in the auditor's judgment, other risk areas which the auditor has identified as an area where the likelihood of material misstatement cannot be reduced to remote, without the need for gaining an understanding of the associated control environment, along with the performance of an appropriate level of substantive work. The risk of misstatement for an RPR is lower than that for a significant risk, and they are not considered to be areas that are highly judgmental, or unusual in relation to the day to day activities of the business.

Risk	Reason for risk identification	Key aspects of our proposed response to the risk
Contributions	Contributions from employers and employees' represents a significant percentage of the Fund's revenue.	<p>We will:</p> <ul style="list-style-type: none"> • evaluate the Fund's accounting policy for recognition of contributions for appropriateness; • gain an understanding of the Fund's system for accounting for contribution income and evaluate the design of the associated controls; • test a sample of contributions to source data to gain assurance over their accuracy and occurrence; • rationalise contributions received with reference to changes in member body payrolls and the number of contributing members to ensure that any unusual trends are satisfactorily explained.
Pension Benefits Payable	Pension benefits payable represents a significant percentage of the Fund's expenditure.	<p>We will:</p> <ul style="list-style-type: none"> • evaluate the Fund's accounting policy for recognition of pension benefits expenditure for appropriateness; • gain an understanding of the Fund's system for accounting for pension benefits expenditure and evaluate the design of the associated controls; • test a sample of individual pensions in payment by reference to member files; • rationalise pensions paid with reference to changes in pensioner numbers and pension increases applied in year to ensure that any unusual trends are satisfactorily explained.

Reasonably possible risks identified

Risk	Reason for risk identification	Key aspects of our proposed response to the risk
The valuation of Level 2 investments is incorrect	While level 2 investments do not carry the same level of inherent risks associated with level 3 investments, there is still an element of judgement involved in their valuation as their very nature is such that they cannot be valued directly.	<p>We will</p> <ul style="list-style-type: none"> • gain an understanding of the Fund's process for valuing Level 2 investments and evaluate the design of the associated controls. • review the reconciliation of information provided by the fund managers, the custodian, the accounting partner (HSBC) and the Fund's own records and seek explanations for variances • consider the competence, expertise and objectivity of any management experts used. • review the qualifications of the expert to value the level 2 investments at year end and gain an understanding of how the valuation of these investment has been reached. • For direct property investments agree values in total to the valuer's report and undertake steps to gain reliance on the valuer as an expert • review the nature and basis of estimated values and consider what assurance management has over the year end valuations provided for these types of investments.

Other matters

Other work

The Fund is administered by [ANOTHER Council] (the 'Council'), and the Fund's accounts form part of the Council's financial statements. Therefore as well as our general responsibilities under the Code of Practice a number of other audit responsibilities also follow in respect of the Fund, such as:

- We consider our other duties under the Act and the Code, as and when required, including:
 - giving electors the opportunity to raise questions about your 2017/18 financial statements, consider and decide upon any objections received in relation to the 2017/18 financial statements;
 - issue of a report in the public interest; and
 - making a written recommendation to the Council, copied to the Secretary of State.
- We carry out work to satisfy ourselves on the consistency of the Fund's financial statements included in the Fund's annual report with the audited Fund accounts.

Other material balances and transactions

Under International Standards on Auditing, "irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance and disclosure". All other material balances and transaction streams will therefore be audited. However, the procedures will not be as extensive as the procedures adopted for the risks identified in this report.

Going concern

As auditors, we are required to "obtain sufficient appropriate audit evidence about the appropriateness of management's use of the going concern assumption in the preparation and presentation of the financial statements and to conclude whether there is a material uncertainty about the entity's ability to continue as a going concern" (ISA (UK) 570). We will review management's assessment of the going concern assumption and evaluate the disclosures in the financial statements.

Materiality

The concept of materiality

The concept of materiality is fundamental to the preparation of the financial statements and the audit process and applies not only to the monetary misstatements but also to disclosure requirements and adherence to acceptable accounting practice and applicable law. Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Materiality for planning purposes

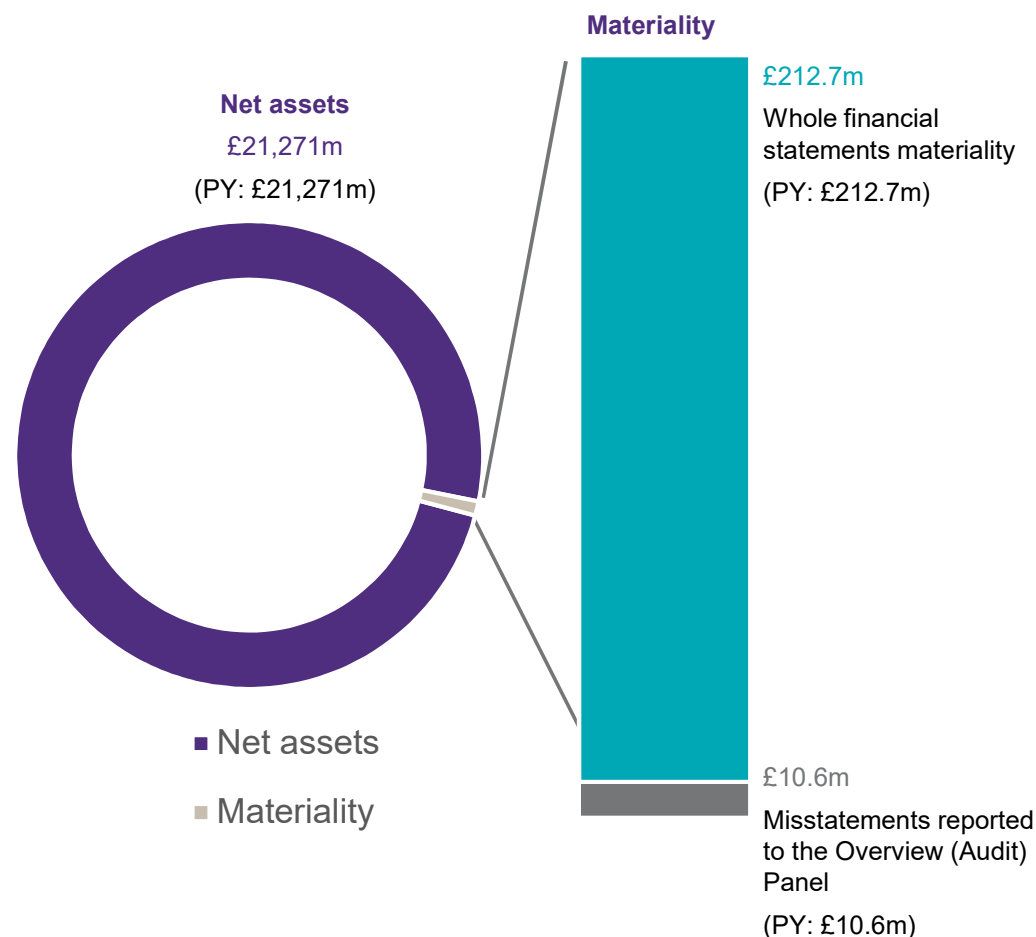
We propose to calculate financial statement materiality based on a proportion of the net assets of the Fund for the financial year. In the prior year we used the same benchmark. We have determined planning materiality (the financial statements materiality determined at the planning stage of the audit) to be £212.7m (PY £212.7m), which equates to 1% of your net assets for the prior year. We design our procedures to detect errors in specific accounts at a lower level of precision.

We reconsider planning materiality if, during the course of our audit engagement, we become aware of facts and circumstances that would have caused us to make a different determination of planning materiality

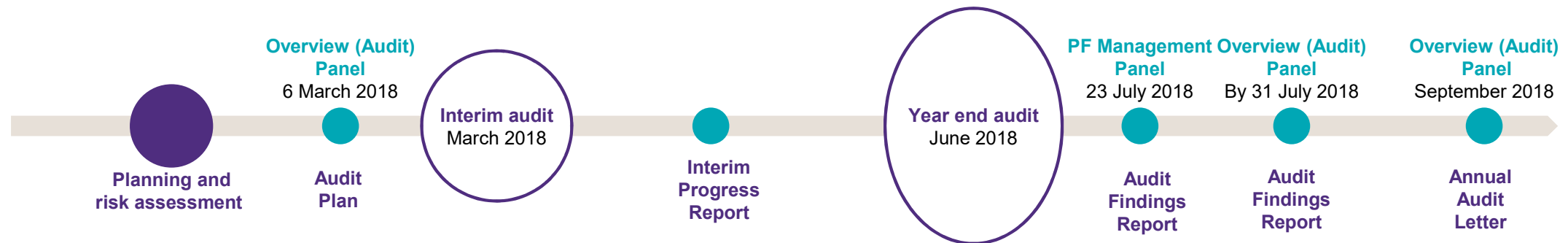
Matters we will report to the Overview (Audit) Panel

Whilst our audit procedures are designed to identify misstatements which are material to our opinion on the financial statements as a whole, we nevertheless report to the Overview (Audit) Panel any unadjusted misstatements of lesser amounts to the extent that these are identified by our audit work. Under ISA 260 (UK) 'Communication with those charged with governance', we are obliged to report uncorrected omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. ISA 260 (UK) defines 'clearly trivial' as matters that are clearly inconsequential, whether taken individually or in aggregate and whether judged by any quantitative or qualitative criteria. In the context of the Fund, we propose that an individual difference could normally be considered to be clearly trivial if it is less than £10.6 m (PY £10.6 m).

If management have corrected material misstatements identified during the course of the audit, we will consider whether those corrections should be communicated to the Overview (Audit) Panel to assist it in fulfilling its governance responsibilities.



Audit logistics, team & audit fees



Mike Thomas, Engagement Lead

Mike will be the main point of contact for the, Section 151 Officer and Senior Pension Fund Executives as well as elected members.. Mike will share his knowledge and experience across the sector and ensure our audit it tailored specifically to you and is delivered efficiently. Mike will review all reports and the team's work.



Marianne Dixon, Audit Manager

Marianne will be responsible for overall management of the audit; quality assurance and quality of audit work and outputs. Marianne will attend key Management Panel meetings as well as Overview (Audit) Panel meetings and draft reports to make sure they are clear, concise and understandable to all.



Mark Stansfield, Audit Incharge

Mark will lead the onsite team and will be the day to day contact for the audit. Mark will monitor the deliverables, manage the query log with your finance team and highlight any significant issues and adjustments to senior management. Mark will undertake the more technical aspects of the audit and coach the junior members of the team.

Audit fees

The planned audit fees are no less than £56,341 (PY: £56,341) for the financial statements audit and £5,996 for the provision of IAS 19 reports to PSAA appointed auditors. In setting your fee, we have assumed that the scope of the audit, and the Fund and its activities, do not significantly change.

Where requests are received from other auditors of other bodies for assurance in respect of information held by the Fund and provided to the actuary to support their individual IAS 19 calculations these will be billed in addition to the audit fee on a case by case basis.

Grant Thornton UK LLP also provides audit services to:

- Matrix Homes Limited Partnership for audit fees totalling £10,000*;
- Plot 5 First Street GP Limited and Plot 5 First Street Partnership Limited for audit fee of £11,000*
- GLIL Infrastructure LLP for audit fee of £8,240*;
- GLIL Corporate Holdings Limited for audit fee of £2,000*
- GMPF Unit Trust £7,450*

These are separate engagements outside the remit of Public Sector Audit Appointments Limited. (* based on 2016/17 audit fees)

Our requirements

To ensure the audit is delivered on time and to avoid any additional fees, we have detailed our expectations and requirements in the following section 'Early Close'. If the requirements detailed overleaf are not met, we reserve the right to postpone our audit visit and charge fees to reimburse us for any additional costs incurred.

Early close

Meeting the early close timeframe

Bringing forward the statutory date for publication of audited local government accounts to 31 July this year, across the whole sector, is a significant challenge for local authorities and auditors alike. For authorities, the time available to prepare the accounts is curtailed, while, as auditors we have a shorter period to complete our work and face an even more significant peak in our workload than previously.

We have carefully planned how we can make the best use of the resources available to us during the final accounts period. As well as increasing the overall level of resources available to deliver audits, we have focused on:

- Page 250
- bringing forward as much work as possible to interim audits
 - starting work on final accounts audits as early as possible, by agreeing which authorities will have accounts prepared significantly before the end of May
 - seeking further efficiencies in the way we carry out our audits
 - working with you to agree detailed plans to make the audits run smoothly, including early agreement of audit dates, working paper and data requirements and early discussions on potentially contentious items.

We are satisfied that, if all these plans are implemented, we will be able to complete your audit and those of our other local government clients in sufficient time to meet the earlier deadline.

Client responsibilities

Where individual clients do not deliver to the timetable agreed, we need to ensure that this does not impact on audit quality or absorb a disproportionate amount of time, thereby disadvantaging other clients. We will therefore conduct audits in line with the timetable set out in audit plans (as detailed on page 11). Where the elapsed time to complete an audit exceeds that agreed due to a client not meeting its obligations we will not be able to maintain a team on site. Similarly, where additional resources are needed to complete the audit due to a client not meeting their obligations we are not able to guarantee the delivery of the audit by the statutory deadline. Such audits are unlikely to be re-started until very close to, or after the statutory deadline. In addition, it is highly likely that these audits will incur additional audit fees.

Our requirements

To minimise the risk of a delayed audit or additional audit fees being incurred, you need to ensure that you:

- produce draft financial statements of good quality by the deadline you have agreed with us, including all notes
- ensure that good quality working papers are available at the start of the audit, in accordance with the working paper requirements schedule that we have shared with you
- ensure that the agreed data reports are available to us at the start of the audit and are reconciled to the values in the accounts, in order to facilitate our selection of samples
- ensure that all appropriate staff are available on site throughout (or as otherwise agreed) the planned period of the audit
- respond promptly and adequately to audit queries.

In return, we will ensure that:

- we will notify you of a list of deliverables in advance of the audit;
- the audit runs smoothly with the minimum disruption to your staff
- you are kept informed of progress through the use of an issues tracker and weekly meetings during the audit
- we are available to discuss issues with you prior to and during your preparation of the financial statements.

Independence & non-audit services

Auditor independence

Ethical Standards and ISA (UK) 260 require us to give you timely disclosure of all significant facts and matters that may bear upon the integrity, objectivity and independence of the firm or covered persons, relating to our independence. We encourage you to contact us to discuss these or any other independence issues with us. We will also discuss with you if we make additional significant judgements surrounding independence matters.

We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention. We have complied with the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements. Further, we have complied with the requirements of the National Audit Office's Auditor Guidance Note 01 issued in December 2016 which sets out supplementary guidance on ethical requirements for auditors of local public bodies.

We confirm that we have implemented policies and procedures to meet the requirements of the Ethical Standard. For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the Fund.

Non-audit services

No non-audit services have been identified to date

Appendices

Appendix A: Revised ISAs

Detailed below is a summary of the key changes impacting the auditor's report for audits of financial statement for periods commencing on or after 17 June 2016.

Section of the auditor's report	Description of the requirements
Conclusions relating to going concern	We will be required to conclude and report whether: <ul style="list-style-type: none">• The directors use of the going concern basis of accounting is appropriate• The directors have disclosed identified material uncertainties that may cast significant doubt about the Fund's ability to continue as a going concern.
Material uncertainty related to going concern	We will need to include a brief description of the events or conditions identified that may cast significant doubt on the Fund's ability to continue as a going concern when a material uncertainty has been identified and adequately disclosed in the financial statements. Going concern material uncertainties are no longer reported in an Emphasis of Matter section in our audit report.
Other information	We will be required to include a section on other information which includes: <ul style="list-style-type: none">• Responsibilities of management and auditors regarding other information• A statement that the opinion on the financial statements does not cover the other information unless required by law or regulation• Reporting inconsistencies or misstatements where identified
Additional responsibilities for directors and the auditor	We will be required to include the respective responsibilities for directors and us, as auditors, regarding going concern.
Format of the report	The opinion section appears first followed by the basis of opinion section.

