Public Document Pack

Tameside
Metropolitan Borough

ASHTON-UNDER-LYNE · AUDENSHAW · DENTON · DROYLSDEN · DUKINFIELD · HYDE · LONGDENDALE · MOSSLEY · STALYBRIDGE

AUDIT PANEL

Day:	**Tuesday**
Date:	**1 November 2016**
Time:	**2.00 pm**
Place:	**Lesser Hall - 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 31 May 2016 to be signed by the Chair as a correct record (Minutes attached).	1 - 6
4.	**PROGRESS REPORT ON RISK MANAGEMENT AND INTERNAL AUDIT ACTIVITIES APRIL TO SEPTEMBER 2016** To consider a report of the Assistant Executive Director (Finance).	7 - 60
5.	**LOCAL AUDIT AND ACCOUNTABILITY ACT 2014** To consider a report of the Assistant Executive Director (Finance).	61 - 68
6.	**RISK MANAGEMENT** To consider a report of the Assistant Executive Director (Finance).	69 - 80
7.	**URGENT ITEMS** To consider any additional items the Chair is of the opinion shall be dealt with as a matter of urgency.	

From: Democratic Services Unit – any further information may be obtained from the reporting officer or from Charlotte Forrest on charlotte.forrest@tameside.gov.uk or 0161 342 2346, to whom any apologies for absence should be notified.

This page is intentionally left blank

AUDIT PANEL

Tuesday, 31 May 2016

Commenced: 2.00 pm **Terminated:** 3.00 pm

Present:	Councillors Ricci (Chair), Ryan (Deputy Chair), Bailey, Buckley, Fairfoull, J Fitzpatrick and Peet
Apologies for Absence:	Councillor Welsh

1. DECLARATIONS OF INTEREST

There were no declarations of interest.

2. MINUTES

The Minutes of the proceedings of the meeting of the Audit Panel held on 1 March 2016 were agreed and signed as a correct record.

3. ACCOUNTING POLICIES AND ESTIMATES FOR 2015/16 ACCOUNTS

Consideration was given to a report of the Assistant Executive Director (Finance), which sought to bring certain items to the attention of the Panel in advance of the closure of the accounts for 2015/16, as follows:

- 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 (IFRS), were used to produce the financial statement for 2015/16 and were appended to the report.

The key change with regard to the policies in respect of 2015/16 had been the adoption of IFRS13 Fair Value Measurement and the introduction of the concept of current value. The Code required the change that non-operational property, plant and equipment classified as surplus assets be measured at fair value. Local Authorities were required to apply the fair value measurements and additional disclosures from 1 April 2015.

Judgements to be used in preparing the accounts were detailed and included accounting for schools (balance sheet recognition of schools and transfers to academy status), investment properties and property plant and equipment. Particular reference was made to accounting for schools transfer to academy status.

RESOLVED:

(i) That the amended Statement of Accounting Policies, as appended to the report, be agreed; and

(ii) That the critical judgements and major sources of estimated uncertainties included within the Statement of Accounts and the impact of alternative estimation bases being used, be noted.

4. AUDIT PLAN

The Panel welcomed representatives of Grant Thornton, External Auditor, who presented their audit plan for Tameside MBC and GMPF for the year ending March 2016.

a TMBC Audit Plan

Stephen Nixon, Grant Thornton, presented the audit plan for TMBC. The report outlined the challenges and opportunities the Council was facing and considered the impact of developments in the sector, whilst taking account of national audit requirements as set out in the Code of Audit Practice.

The audit approach was highlighted including the focus on risk with any significant and other risks identified. The result of interim audit work was detailed alongside key dates of the audit cycle and value for money. Panel Members were notified that there were no significant risks identified as part of value for money risk assessment and planning.

RESOLVED
That the audit plan be noted.

b GMPF Audit Plan

Mike Thomas, Grant Thornton, presented the audit plan for GMPF. The report outlined the challenges and opportunities the Pension Fund was facing and considered the impact of developments in the sector, whilst taking account of national audit requirements as set out in the Code of Audit Practice.

The audit approach was highlighted including the focus on risk with any significant and other risks identified. The result of interim audit work was detailed alongside key dates of the audit cycle.

RESOLVED
That the audit plan be noted.

5. AUDIT FEE LETTER

Consideration was given to the audit fee letter from Grant Thornton for the external audit of 2016/17.

It was reported that the Public Sector Audit Appointments Limited (PSAA) would oversee the Commission's audit contracts for local government bodies until they ended in 2018. Their responsibilities included setting fees, appointing auditors and monitoring the quality of auditor's work. The PSAA prescribed that 'scale fees are based on the expectation that audited bodies are able to provide the audit with complete and materially accurate financial statements, with supporting papers, within agreed timescales'.

The PSAA had proposed that the 2016/17 scale audit fees be set at the same level as the scale fees applicable for 2015/16. The audit planning process for 2016/17, including the risk assessment, would continue as the year progressed and fees would be reviewed and updated as necessary as work progressed.

Audit planning and interim audit procedures would be undertaken from November 2016 to March 2017 and upon completion a detailed audit plan setting out findings and the audit approach would be issued. The final accounts audit and work on the value for money conclusion would be completed in August 2017 and work on the whole of government accounts returned in September 2017.

RESOLVED
That the letter be noted.

6. REVIEW OF INTERNAL AUDIT 2015/16

Consideration was given to a report of the Assistant Executive Director (Finance), which reviewed the effectiveness of internal audit and measured practices and performance of the Internal Audit function with the standards that contributed to the overall effectiveness of the system of internal control.

Information was given with regard to the background to the review, the requirements of the Public Sector Internal Audit Standards, the process that had been adopted and details of the review itself. The standards and an assessment against each of the standards and a comparison of the results for 2015 compared to the position as at March 2016 were detailed.

The report concluded that, against each of the standards, Internal Audit had achieved all the requirements of the Public Sector Internal Audit Standards and that the Internal Audit Service contributed to the overall effectiveness of the system of internal control. The outcome of the review, together with the positive comments received from the External Auditors and also from Senior Management Teams/Executive Members, demonstrated that the Council had an adequate and effective internal audit function.

RESOLVED
That the report be noted.

7. RISK MANAGEMENT AND AUDIT SERVICES - ANNUAL REPORT 2015/16

The Head of Risk Management and Audit Services submitted a report, which summarised the work performed by the Service Unit and provided assurances as to the adequacy of the Council's system of internal control.

The key achievements of the service unit for 2015/16 were highlighted and included 94% of planned audits being delivered and 92% of audit recommendations being implemented.

It was explained that the report presented to the Audit Panel in May 2015 provided an overview of the work planned for 2015/16. The plan, as reported during the year, was revised on a regular basis to ensure that it was aligned to changes in service priorities, risks, directorate structures and resources available.

The full year position of the audit plan by Directorate/Service Area was detailed, which displayed the approved and revised plan for 2015/16, actual days as at 31 March 2015 and the percentage completed. In terms of the overall plan 1,675 actual days were delivered against a revised plan of 1,656.

Examples of the audit work undertaken in each directorate and a summary of the audit opinions issued in relation to system based audit work and also schools for 2015/16, compared to 2014/15 and 2013/14, was provided.

With regard to anti-fraud work, 27 cases had been investigated during the period April 2015 to March 2016 and investigations by fraud type, the value and potential annual savings were provided. Work continued during 2015/16 on the matches identified from the National Fraud Initiative 2014 data matching exercise and the results were summarised.

The report further detailed the following:

- Risk Management and Insurance;
- Performance indicators; and
- Audit opinion based on results of 2015/16 activity.

The report concluded that the overall audit opinion was that the Authority's governance, risk and control framework was generally sound and operated reasonably consistently. It was accepted that the gross risk for the Council had increased in recent years (due to reduced capacity, whilst still having to deliver a significant change programme to meet financial challenges). Controls were in place to mitigate such risks and where improvements had been highlighted, managers had agreed to implement the suggested recommendations. This would aid the management of risk and support the overall control environment.

RESOLVED
That the report be noted.

8. ANNUAL GOVERNANCE REPORT 2015/16

The Assistant Executive Director (Finance) submitted a report, which sought Members' views on the following:

- The Draft Annual Review against the Code of Corporate Governance for 2015/16;
- The Draft Annual Governance Statement for 2015/16; and
- The Draft Code of Corporate Governance for 2016/19.

The report explained an updated version of the Framework *Delivering Good Governance in Local Government* was published at the end of April 2016 to become effective for 2016/17. The core principles of the 2016 framework were outlined.

It was reported that a review had 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 and Statement of Assurance, which were required by the Accounts and Audit Regulations 2015. The draft Annual Review for 2015/16 was appended to the report.

The draft Annual Governance Statement for 2015/16 and the draft Code of Corporate Governance for 2016/19 were also appended to the report for comment.

RESOLVED
(i) That the draft Annual Review against the Code of Corporate Governance for 2015/16 be approved;
(ii) That the draft Annual Governance Statement for 2015/16 be approved;
(iii) That the draft Code of Corporate Governance for 2016/19 be approved; and
(iv) That delegated authority be granted to the Assistant Executive Director (Finance) to make further amendments to the Draft Annual Governance Statement upon receipt of further comments.

9. RISK MANAGEMENT AND AUDIT SERVICES PLANNED WORK 2016/17

Consideration was given to a report of the Assistant Executive Director (Finance), which presented the planned work for the Risk Management and Audit Service for 2016/17. The report set out in detail the work of Internal Audit and sought approval for the Annual Audit Plan for 2015/16, which was appended to the report.

The Head of Risk Management and Audit Services explained that the Plan was reviewed and revised each year to take into account service and legislative changes, which could result in large shifts in priorities and culminated in the production of the Annual Audit Plan.

It was reported that Audits were prioritised based on an assessment of risk and allocated a risk score of High, Medium/High, Medium, Low/Medium or Low and the factors taken into account were outlined.

The Annual Plan for 2016/17 was appended to the report and the report provided a summary of the key audits to be undertaken in each Directorate, including those planned for the Greater Manchester Pension Fund. The total days required to deliver the plan were 1,798 days and had been matched to available resources. It was further reported that the Plan would be kept under constant review and regular meetings would be held with the Senior Management Team to ensure that it truly reflected the key risks for the Council going forward as it changed in shape and size to meet the financial challenges placed upon it.

It was reported that a self-assessment against the Public Sector Internal Audit Standards (PSIAS) had been completed to inform the Review of the Effectiveness of the System of Internal Control and the service was fully compliant with the Standards. An external assessment must be conducted at least once every five years as part of the PSIAS and this would be conducted by members of the North West Chief Audit Executive Group during the next two years.

A self-assessment against the Chartered Institute of Public Finance and Accountancy (CIPFA) Statement for the Head of Internal Audit had also been completed as part of the review and the assurance work for the preparation of the Annual Governance Statement. The Head of Risk Management and Audit Services was compliant with all the requirements.

In order to comply with PSIAS, it was necessary for the Audit Panel to approve the Internal Audit Strategy and the Internal Audit Charter, both of which were also appended to the report.

The report further detailed the following:

- Quality assurance and improvement programme;
- Proactive fraud work/irregularity investigations;
- Risk management and insurance;
- National Anti-Fraud Network Data and Intelligence Services;
- Performance Monitoring; and
- Member Training.

RESOLVED
(i) That the draft Internal Audit Annual Plan for 2016/17 be approved;
(ii) That the Internal Audit Strategy for 2016/17 be approved;
(iii) That the Internal Audit Charter for 2016/17 be approved; and
(iv) That the Quality Assurance and Improvement Programme for 2016/17 be approved.

10. RISK MANAGEMENT

The Assistant Executive Director (Finance) submitted a report, which presented the Risk Management Policy and Strategy for 2016/17 and the Corporate Risk Register, as appended to the report.

It was explained that Risk Management was the process of identifying risks, evaluating their likelihood and potential impact and determining the most effective methods of controlling them or responding to them. It was a means of maximising opportunities and minimising the costs and disruption to the organisation caused by undesired events.

The benefits of risk management were identified. It was explained that the Council recognised that it was the responsibility of all Members and employees to have regard for risk in carrying out their duties. If uncontrolled, risk could result in a drain on resources that could better be directed to front line service provision and to the meeting of the Council's objectives and community needs.

It was further explained that the Risk Management Policy and Strategy had been reviewed and updated and a copy was appended to the report.

A copy of the Corporate Risk Register was also appended to the report. A list of risks had been removed as they had been successfully managed and new risks had been added to the register. Particular reference was made to the impact on the Council in relation to the changing landscape for schools.

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

11. GMPF STATEMENT OF ACCOUNTS 2014-2015 GOVERNANCE ARRANGEMENTS

The Assistant Director of Pensions (Local Investments and Property) presented a report informing Members 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. The report also sought Members approval of the key assumptions for estimates to be used in the accounts.

It was explained that the key decision making bodies for the Council were the Audit Panel, which received accounting policy reports for both GMPF and the Council, and the Overview (Audit) Panel, which received the report of the external auditor following the audit of the accounts. TMBC retained overall responsibility for the accounts of both and the follow-up on the audit reports received for both, but in practice delegated the responsibility for GMPF to GMPF.

The provisional timetable for approval of the accounts and audit reports by these bodies for 2016/17 was outlined in the report.

The key continuing assumptions used in production of the accounts included accruals basis, fair value for investments, liabilities in compliance with International Accounting Standard 19 and continued phased implementation of CIPFA's guidance on accounting for management costs in the Fund. Particular reference was made to fair valuations.

RESOLVED
(i) That the governance arrangements for approval of GMPF accounts be noted; and
(ii) The assumptions for estimates to be used in the GMPF Accounts be approved.

12. URGENT ITEMS

The Chair reported that there were no urgent items for consideration at the meeting.

CHAIR

Agenda Item 4.

Report To:	**AUDIT PANEL**
Date:	1 November 2016
Reporting Officer:	Ian Duncan – Assistant Executive Director (Finance) Wendy Poole – Head of Risk Management and Audit Services
Subject:	**PROGRESS REPORT ON RISK MANAGEMENT AND INTERNAL AUDIT ACTIVITIES APRIL TO SEPTEMBER 2016**
Report Summary:	To advise members of the work undertaken by the Risk Management and Internal Audit Service between April and September 2016 and to comment on the results.
Recommendations:	1. That members note the report and the performance of the Service Unit for the period April to September 2016. 2. Members approve the Information Governance Policy at **Appendix 1**. 3. Members approve the Information Governance Conduct Policy at **Appendix 2**. 4. Members approve the Information Security Incident Reporting Procedure/Practice Note at **Appendix 3**. 5. Members approve the Subject Access Requests Guidance at **Appendix 4**. 6. Members support the Peer Review process for the Assessment of Internal Audit outlined in **Section 4** of 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 reducing losses due to poor risk management. It also helps to keep insurance premiums and compensation payments 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:	Assists in providing the necessary levels of assurance that the significant risks relating to the council's operations are being effectively managed.

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 This is the first progress report for the current financial year and covers the period April to September 2016.

1.2 The main objective of this report is to summarise the work undertaken by the Risk Management and Internal Audit Service during the first half of the year in respect of the approved Plan for 2016/2017, which was presented to the Audit Panel in May 2016.

2. RISK MANAGEMENT AND INSURANCE

2.1 The Risk Management and Insurance Team provide services to the whole Council including schools. The key priorities for the team during 2016/2017 are:-

To review the risk management system and

- facilitate the delivery of risk workshops for managers to enable risk registers to be updated.
- To facilitate the continued implementation of the Information Governance Framework by:-
  - Providing advice and guidance in relation to information governance;
  - Keeping the framework up to date and fit for purpose with any new guidance issued by the Information Commissioners Office (ICO);
  - Delivering and monitoring training for general users and for staff in high risk areas.
- To review the Business Continuity Management system in place to streamline the process to create a management tool that is workable, with a capability to provide knowledge and information should a major incident occur.
- 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.

2.2 The risk management system is under review. The Corporate Risk Register is now presented to the Senior Management Team on a quarterly basis and a separate report is on the agenda presenting the October update to the Panel. During quarter three operational risk registers will be compiled by service areas using the corporate risk register template and this will be facilitated by the Head of Risk Management and Audit Services.

2.3 With regards to Information Governance Framework a number of the documents have been revised to take into account some minor structural or procedural changes as follows:-

- Information Governance Policy – Updated to reflect structural changes and the addition of the revised Subject Access Request Guidance, see **Appendix 1**.
- Information Governance Conduct Policy – Updated to reflect the additional Subject Access Request Guidance, see **Appendix 2**.
- Information Security Incident Reporting Procedure – Updated to reflect some structural changes and to include a practice note for undertaking investigations, see **Appendix 3**.
- Subject Access Requests Guidance – Refreshed to ensure consistency across all areas of the Council, see **Appendix 4**.

2.4 Business Continuity Management will be assessed as part of the work undertaken with service areas to identify Operational Risk Registers as a methodology that is fit for purpose needs to be established.

3. INTERNAL AUDIT

3.1 The Audit Plan approved on 31 May 2016 covered the period April 2016 to March 2017 and totalled 1,798 Days. This was made up of 1,323 days on planned audits and 475 days on reactive fraud work.

3.2 Table 1 below provides an update on progress against the plan to 30 September 2016. The actual days delivered at quarter 2 are 761, which equates to 42% of the total audit days planned for 2016/17 at 1,798, compared to 41% at this stage during 2015/16, 50% in 2014/15 and 45% in 2013/14.

3.3 The table below shows how the audit plan is profile across the year and demonstrates that at the end of Quarter 2 Internal Audit have delivered 117 days short of the planned target of 878 days. Performance to date has been affected by reduced resources, annual leave and ad hoc requests for reviews, advice and support, which were not included in the original plan that were a greater priority in relation to the planned work. The Audit Plan is responsive to the needs of the organisation and as such it is normal practice to review and amend the plan during the year.

3.4 An Auditor left at the beginning of June and one of the Fraud Investigators/counter fraud Specialists left at the end of August. Recruitment has been completed and a new Auditor has recently started with the team and the new Fraud Investigator will take up post in November.

3.5 **Table 1 – Annual Audit Plan Progress as at 30 September 2016**

Service Area / Directorate	2016/17 Plan	2016/17 Q1/Q2 Profile	2016/17 Actual Days Q2	2016/17 Q2 Variance	2016/17 Q3/Q4 Days to Deliver
People	250	172	141	-31	108
Public Health	51	30	22	-8	21
Place	222	98	75	-23	139
Governance and Resources	262	125	93	-32	167
Schools	175	80	76	-4	113
Cross Cutting	63	39	21	-18	24
Greater Manchester Pension Fund	300	97	95	-2	203
Planned Days 2016/17	**1,323**	**641**	**523**	**-118**	**775**
Proactive Fraud Work and Irregularity Investigations	475	237	238	1	238
Total Days 2016/17	**1,798**	**878**	**761**	**-117**	**1,013**

3.6 A detailed review of the audit plan is currently underway in conjunction with senior management to ensure that the plan is still relevant and meets with available resources in the team. The original plan of 1,798 days which represented planned work was based on estimated resources at the beginning of the year. A revised plan will be reported to a future meeting of the Panel.

3.7 During the first half of the year, 10 Final Reports were issued in relation to systems, risk and managed audits, the results of which are summarised in table 2 below.

Table 2 – Final Reports Non-Schools

Opinion	Number	%	Total To Date	Total for 2015/16
High	1 (1)	11	1 (1)	6 (4)
Medium	8 (5)	78	8 (5)	14 (3)
Low	1 (1)	11	1 (1)	5 (0)
Totals	**10 (7)**	**100**	**10 (7)**	**25 (7)**

Note: The figures in brackets relate to Final Reports issued for the Pension Fund.

3.8 In addition to the final reports issued above, 7 Draft Reports have been issued for management review and responses and these will be reported to the Panel in due course.

3.9 Not all work undertaken by the team generates an audit opinion and several pieces of work undertaken in the period fall into this category:-

- Hattersley Collaboration Agreement
- Public Health Grant
- Local Transport Settlement Grant
- Troubled Families Financial Claim Verification
- Pension Scheme Verification Checks
- Bus Subsidy and Pinchpoint Grants
- Terms and Conditions Assurance work
- Pension Fund – Valuation Assurance Work

3.10 2 School Audits were completed during the period, the results of which are summarised in table 3 below.

Table 3 – Final Reports Schools

Opinion	Number	%	Total To Date	Total for 2015/16
High	1	50	1	9
Medium	1	50	1	7
Low	0	0	0	5
Totals	**2**	**100**	**2**	**21**

3.11 In addition to the final reports issued above, 6 visits have been completed and the draft reports are being reviewed before they are issued to the Schools for management review and responses and these will be reported to the Panel in due course.

3.12 Post Audit Reviews are undertaken approximately six months after the Final Report has been issued, however, where a low level of assurance is issued the post audit review is scheduled for three months to ensure that the issues identified are addressed. 8 Post Audit Reviews have been completed during the period. Internal Audit was satisfied with the reasons put forward by management where the recommendations had not yet been fully implemented. A further 12 Post Audit Reviews are in progress, which will be reported to the Panel at a future meeting.

4. REVIEW OF INTERNAL AUDIT

4.1 The review of Internal Audit reported to the Audit Panel on 31 May 2016 against the Public Sector Internal Auditing Standards (PSIAS) highlighted that the service is fully compliant with the requirements of the standard.

4.2 The Public Sector Internal Audit Standards (PSIAS), introduced from April 2013, require at Standard 1312 that each organisation's internal audit service is subject to an external assessment "once every five years by a qualified, independent assessor or assessment team from outside the organisation".

4.3 Across AGMA and the wider North West a Peer Review process has been developed by the Chief Audit Executive Group and piloted in Blackburn and Blackpool. The feedback from both the reviewers and those being assessed is summarised below:-

- The greatest value from the peer review process is the sharing of information and best practice which would otherwise not be gained through an external assessment from an external provider;
- Directors and Audit Committee Chairs value the shared knowledge and experience of other Councils;
- Benchmarking information could be collated and shared across the region
- Being reviewed by professionals in a similar role, facilitates understanding of the issues facing the team under review;
- Teams under review are open in describing the issues they face to fellow professionals; and
- A suite of standard working papers have been developed for consistency including interview questions tailored for Directors/Members.

4.4 Three options have been considered and are detailed in table 4 below.

Table 4 – External Assessment Providers and Costs

Provider	Costs
Local Authority Peer Review	No direct costs. Reciprocal time to undertake reviews
Chartered Institute of Public Finance and Accountancy	£900 per day Estimated to take 4-6 days (£3,600 - £5,400)
Chartered Institute of Internal Auditors	Full External Assessment £14,300 Validated Self-Assessment £11,700

4.5 Evaluation by the Chief Audit Executive Group supported the Peer Review Process. All members of the group were asked to consult their Section 151 Officer during July/August and the Peer Review process was supported overwhelmingly. This was ratified by the Greater Manchester Treasurers at their meeting on 12 August 2016. Currently the programme of reviews is being compiled, however, as we are in the process of upgrading our audit management system Galileo, we have requested a review during the latter part of 2017.

4.6 The Audit Panel is therefore requested to support this option for the Council.

5. ANNUAL GOVERNANCE STATEMENT 2015/16

5.1 The Annual Governance Statement presented to the Audit Panel on 31 May 2016 and approved by the Overview (Audit) Panel on 12 September 2016 highlighted four areas for development. Table 5 below provides an update on progress to date.

5.2 **Table 5 – Annual Governance Statement Development Areas**

Development	Progress to Date
The ongoing level of change across the organisation, reduced resources and staff capacity to deliver the challenges faced by the Council is managed by ensuring that proper governance procedures and risk management are in place to safeguard that the overall control environment is not adversely affected.	A risk based Internal Audit plan is in place which addresses the keys risks facing the council. Risk management is embedded in service delivery as all reports submitted for decisions by both officers and members have to detail the risk implications to ensure that they are being managed. Assistance from Risk Management and Audit is provided when requested. The Corporate Risk Register is reviewed quarterly by Senior Management Team.
As we move towards an Integrated Care Organisation it is critical that strong governance arrangements are in place to ensure that positive outcomes are achieved through robust systems and procedures that are open and transparent and monitored accordingly.	Ongoing meetings are taking place to ensure that strong governance arrangements are introduced. The Internal Auditors for both the Council and the Clinical Commissioning Group are involved in reviewing progress. The Chief Executive has been appointed as the Accountable Officer for the NHS Tameside and Glossop Clinical Commissioning Group. Joint management meetings are now scheduled.
Vision Tameside, which is a multi-million pound project in partnership with Tameside College, is delivered in accordance with agreed milestones and 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.	Regular reports are provided to the Senior Management Team, Board and Cabinet. A project board meets regularly.
Greater Manchester Pension Fund is working with other large metropolitan LGPS funds to create a £35 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.	The Fund has chosen pooling partners and submitted a response to Government. Feedback is awaited and will inform future actions. Professional advice will be sought throughout process.

6. IRREGULARITIES/COUNTER FRAUD WORK

6.1 Fraud, irregularity and whistle-blowing 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.

6.2 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.

6.3 The number of cases investigated during the period April to September 2016 is summarised in Table 6 below.

Table 6 – Investigations Undertaken from April to September 2016

Detail	No. of Cases
Cases B/Forward from 2015/2016	12
Current Year Referrals	7
Total	**19**
Cases Closed	6
Cases Still under Investigation	13
Total	**19**
Assistance Cases	**1**

6.4 Joint working between Internal Audit, Legal and Exchequer Services has led to a recent court success where a man was found guilty of fraudulently spending £53,937, which he had claimed to cover care costs. He pleaded guilty at the Magistrates Court on 28 September and has been referred to Crown Court for sentencing on 3 November 2016.

6.5 Work has continued during the period to prepare for the National Fraud Initiative 2016 Data Matching Exercise. Data has now been extracted and uploaded to the Cabinet Office website and matches will be released for investigation in Jan/Feb 2017. The preparation work to achieve this has been coordinated by Internal Audit to ensure that the correct data was extracted and that appropriate Fair Processing Notices were in place as prescribed by the guidance notes issued by the Cabinet Office. Update reports will be provided to the Panel once the data is available.

7. NATIONAL ANTI FRAUD NETWORK DATA AND INTELLIGENCE SERVICES

Interception of Communications Commissioners Office

7.1 The National Anti-Fraud Network provides a Single Point of Contact Service for local authority members to acquire communications data under the Regulatory Investigatory Powers Act 2000 (RIPA). In November 2012 the Home Office required that every local authority accessing this data must use the National Anti-Fraud Networks service.

7.2 The Interception of Communication Commissioner (IoCCO) is responsible for reviewing the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. They report to the Prime Minister on a half-yearly basis.

7.3 The National Anti-Fraud Network is subject to annual inspections by IOCCO and once again emerged with distinction from its recent assessment. The inspectors, who have previously praised the National Anti-Fraud Network, as providing a Rolls Royce service, stated their satisfaction that statutory duties were being carried out responsibly, and the guardian and gatekeeper duties performed effectively. Overall they said very high standards were being achieved. Their recommendations can be found in table 7 below.

Table 7 – Recommendations from the June 2016 Inspection

Recommendation	Achieved (Yes/No/ Partly)	Description / Comments
It is recommended that all Designated Persons should follow the good practice guidance by tailoring their comments to the individual applications as this is the best means of demonstrating that they have been properly considered. If the Single Point of Contacts identify any Designated Persons who are not tailoring their written considerations to the individual applications, then appropriate advice should be provided to assist such Designated Persons to improve the quality of their considerations and make them more robust and immune to challenge. This should also be brought to the attention of National Anti-Fraud Network Single Point of Contact management.	Yes	A circular has been issued to all designated persons and senior responsible officers (attached) highlighting the need to clearly demonstrate considerations when authorising applications. All National Anti-Fraud Network Single Point of Contacts have been instructed to carefully review Designated Person comments and where necessary provide advice and guidance. All instances where advice and guidance is provided are to be reported to the Service Team Manager and escalated where appropriate.
National Anti-Fraud Network should undertake a detailed review of all instances where a delay is occurring between submission of the court pack and judicial approval to identify reasons for delay.	Yes	A centralised register will be maintained for the recording of all submissions to court including number of days taken to obtain judicial approval, reason for judicial delay (where it exceeds 5 working days). All Single Point of Contacts are required to maintain the register which is reviewed weekly by the Service Team Manager.

7.4 The National Anti-Fraud Network has significantly enhanced its profile within central and local government. It is an influential member of several national boards including the Communication Data Strategy Board, Professional Oversight Board for communication data training and accreditation, Communications Data Operational Group and Communications Data and Lawful Interception Strategy Group. The National Anti-Fraud Network also Chair and host the National Training and Best Practice Work Group for non-law enforcement agencies involved in the acquisition of communications data.

7.5 The National Anti-Fraud Network have played an integral role in the introduction of the Investigatory Powers Bill and is recognised as a key stakeholder by the Home Office.

Performance

7.6 During the first six months of 2016/17 the team continue to process data and intelligence requests received from member local authorities, housing associations and other public sector bodies.

7.7 The appointment of a Project Manager in May 2016 has provided the capacity to recommence system development in line with the approved business plan.

7.8 Membership is stable but with increase in shared services it is acknowledged there is a need to wider promote the services, maximise corporate awareness and sustain targeted marketing campaigns. Currently, the team have limited skills and expertise in this area and the Executive Board are responding accordingly.

7.9 A national programme of Roadshows successfully delivered 12 events in Glasgow, Preston, Birmingham, Cardiff, London and Cheltenham to almost 1,000 users. From the survey conducted an overwhelming number of delegates (85%) indicated how beneficial the training received was to their area of work.

7.10 The 2016 AGM and Summit is being hosted at the Royal York Hotel in York on 30 November 2016. The theme of the event is Improving Performance and Outcomes and the speakers are practitioners who will share learning and best practice in relation to Cyber Crime, Empty Property, Social Media and Right to Buy investigations.

7.11 Table 8 below, shows the number of requests received for the period April to September 2016 compared to the two previous years.

Table 8 – Performance Figures for NAFN April to September 2016

Type Of Request	April to Sept 2016/17	April to Sept 2015/16	April to Sept 2014/15	% Increase (Decrease)
General	23,818	34,960	35,561	(32)
SSFA	0*	9,043	31,828	**N/A**
CTRS	1,787	1,003	27	78
POSHFA	2,309	1,978	1,099	17
DVLA	7,911	7,219	12,270	10
RIPA	505	544	2,071	(7)
Online Requests	27,971**	29,670	26,371	(6)
TOTALS	**64,301**	**84,417**	**109,227**	**(24)**

*Transfer of housing benefit investigations to DWP SFIS completed March 2016

**The decrease in use is due to the withdrawal of Equifax Direct service which will be replaced by Equifax PSG Direct. Scheduled go-live October 2016

7.12 The reduction in the number of requests received reflects the introduction of the DWP Single Fraud Investigation Service and the increase in shared services across the country.

8. LOCAL AUDIT AND ACCOUNTABILITY ACT 2014

8.1 A separate report is on the agenda regarding the changes to the procurement of External Auditors introduced by the Local Audit and Accountability Act 2014.

9. RECOMMENDATIONS

9.1 That members note the report and the performance of the Internal Audit Service for the period April to September 2016.

9.2 Members approve the Information Governance Policy at **Appendix 1**.

9.3 Members approve the Information Governance Conduct Policy at **Appendix 2**.

9.4 Members approve the Information Security Incident Reporting Procedure/Practice Note at **Appendix 3**.

9.5 Members approve the Subject Access Requests Guidance at **Appendix 4**.

9.6 Members support the Peer Review process for the Assessment of Internal Audit outlined in section 4 of the report.

This page is intentionally left blank

APPENDIX 1

Information Governance Policy

November 2016

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 Act 1998 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 to organisations for up to £500,000 and £50,000 to individuals for breaches of the Data Protection Act, 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 3 produced in October 2014 by the Public Services Network in partnership with the Local CIO Council, Socitm, the Cabinet Office and the NLAWARP. 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 unathorised 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.

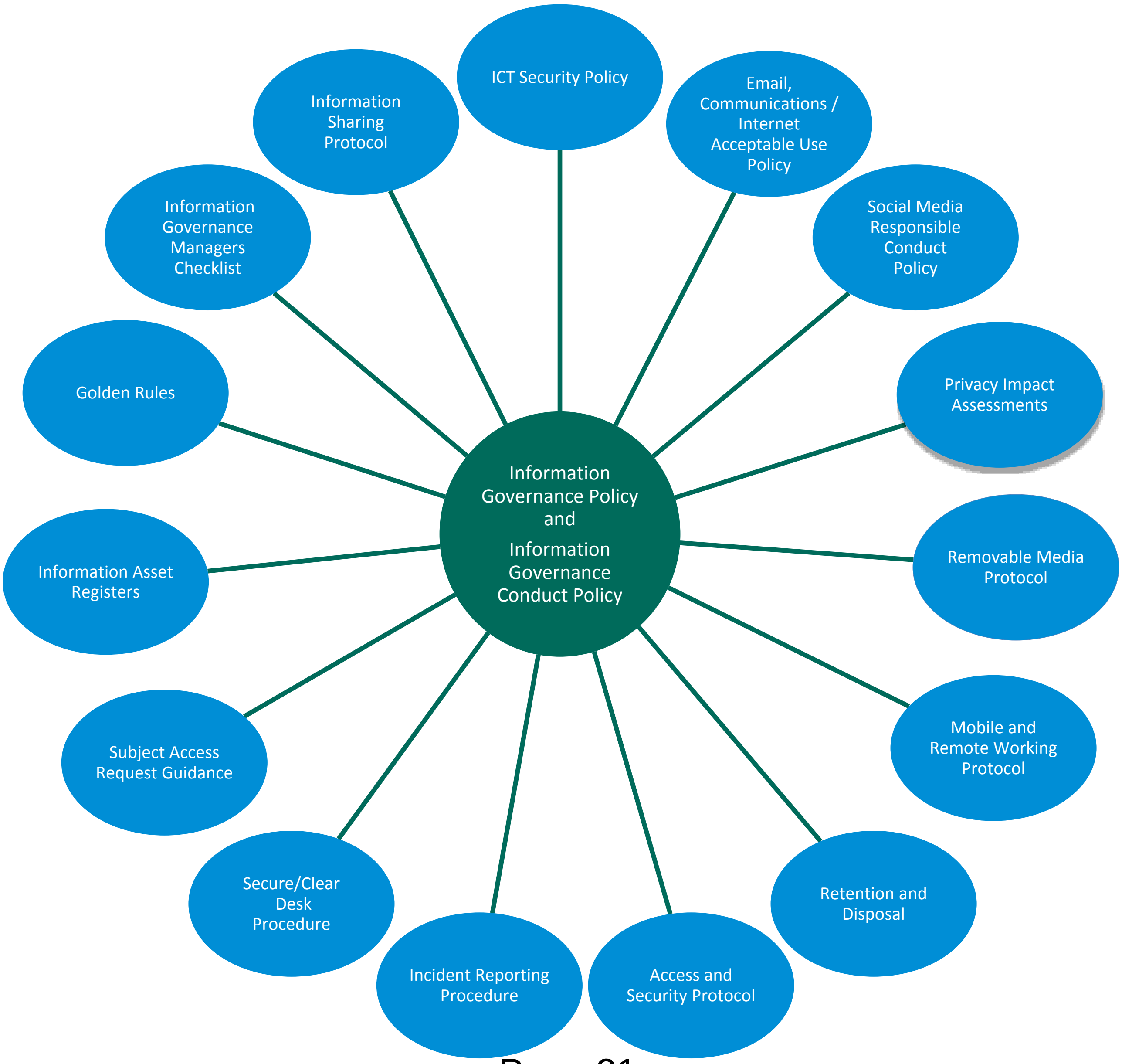
3. INFORMATION GOVERNANCE FRAMEWORK

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;

- Privacy Impact Assessments;
- Removable Media Protocol;
- Mobile and Remote Working Protocol;
- Retention and Disposal ;
- Access and Security Protocol;
- Incident Reporting Procedure;
- Secure/Clear Desk Procedure;
- Subject Access Requests Guidance;
- Information Asset Registers;
- Golden Rules;
- Information Governance Managers Checklist; and
- Information Sharing Protocol.

3.2 Figure 1 – Information Governance Framework


Information Governance Policy and Information Governance Conduct Policy
ICT Security Policy
Email, Communications / Internet Acceptable Use Policy
Social Media Responsible Conduct Policy
Privacy Impact Assessments
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

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 (Executive Directors, Assistant Chief Executives, Assistant Executive 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 2008 and the Local Public Services Data Handling Guidelines 2012 introduce some specific roles in relation to Information Governance as follows:-

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

6.3 These specific roles together with the Data Protection Officer and the IT Security Officer 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. **(Executive Director of Governance, Resources and Pensions)**
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/AEDs 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.

Appendix 1

Information Charter

This Charter is for anyone who has dealings with the Council whether through correspondence, involvement in public policy consultations or if for any other reason we hold personal information about you.

The Charter sets out the standards you can expect when we ask for or hold your personal information and what we ask of you, to help us keep information up to date.

We know how important it is to protect your privacy and to comply with the Data Protection Act 1998.

If we ask for your personal information we promise:

- To make sure you know why we need it;
- To ask only for what we need, and not to collect too much or irrelevant information;
- To protect it and make sure nobody has access to it who should not;
- To let you know if we share it with other organisations to give you better public services – and if you can say no;
- To make sure we don't keep it longer than necessary; and
- Not to make your personal information available for commercial use without your permission. The Council does not sell personal information about customers or correspondents to commercial organisations.

In dealing with your personal information, we will also:

- Value the personal information entrusted to us and make sure we respect that trust;
- Abide by the law when it comes to handling personal information;
- Consider the privacy risks when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- Provide training to employees who handle personal information and respond appropriately if personal information is not used or protected properly.

In return, we ask you to:

- Give us accurate information; and
- Tell us as soon as possible if there are any changes to your circumstances, e.g. a new address

This helps us to keep your information reliable and up to date.

APPENDIX 2

Information Governance Conduct Policy

November 2016

1. Introduction

1.1 Tameside Metropolitan Borough Council (the Council) has a responsibility under the Data Protection Act 1998 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 1998 is the key piece 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 £500,000 for non-compliance.

1.5 The Local Public Services Data Handling Guidelines 2012 outline best practice for protecting information together with resources provided by the Records Management Society, National Archives, Local Authority Information Governance Groups and the 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 the Risk and Insurance Team.

2.4 The table shown in **Appendix 2** identifies the mandatory minimum documents for employees to read relevant to their role. It will be 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 1998, 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 and Insurance Manager 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.

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.

Appendix 1

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 Service Portal and type 'password' in the search box;
- 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. 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 the Data Protection Act 1998 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 of 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 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 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.

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 Act 1998 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 Requests 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. This guidance applies to all employees, including those who may respond to a SAR. It applies to all personal information whether manual, electronic, audio or visual.

Key Conduct Issues

- All subject Access Requests must be dealt with, within the required 40 days.
- All requests must be recorded centrally.
- Documents must be redacted in accordance with guidance issued.

For further guidance (Link to be added when approved)

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 Act 1998 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 trial of all disclosures.

For further guidance click here

Appendix 2

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	✓	✓	✓	✓	✓	✓
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

APPENDIX 3

Information Security Incident Reporting Procedure/Practice Note

November 2016

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 abreach of the Data Protection Act.

Examples of Information Security Incidents have been provided at **Appendix 1.**

Personal information: is any personal data as defined by the Data Protection Act 1998. 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 1998.

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

Protected Informationis any information which is;

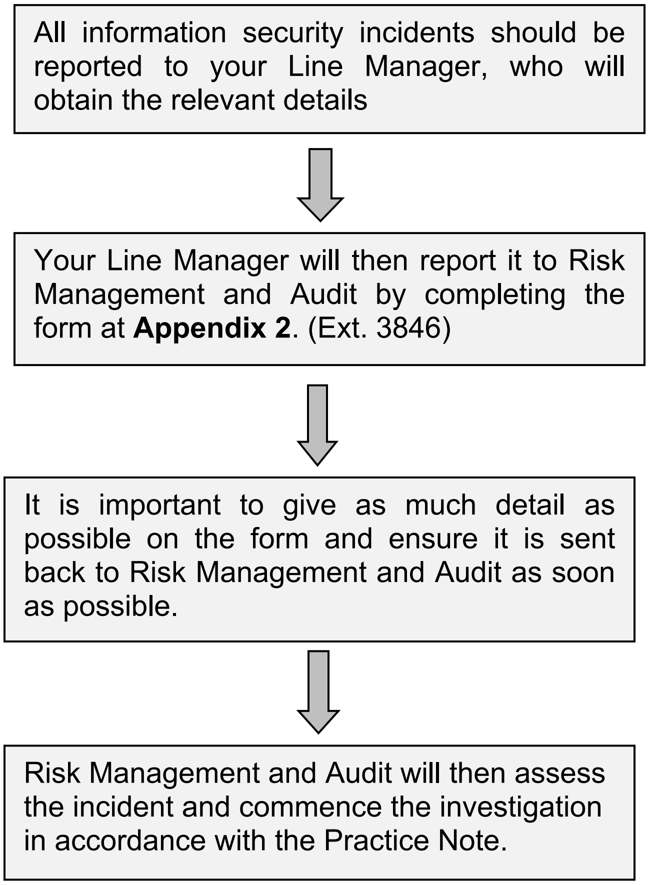
(a) personal/sensitive personal data or
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

3. Roles and Responsibilities

3.1 All employees must understand and adopt the use of this procedure and are responsible for 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 within 24 hours of discovery could result in disciplinary action.

4. Reporting an Incident



All information security incidents should be reported to your Line Manager, who will obtain the relevant details

Your Line Manager will then report it to Risk Management and Audit by completing the form at **Appendix 2**. (Ext. 3846)

It is important to give as much detail as possible on the form and ensure it is sent back to Risk Management and Audit as soon as possible.

Risk Management and Audit will then assess the incident and commence the investigation in accordance with the Practice Note.

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 breach and recover any losses. Action may also be needed to prevent another breach 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
- prevent a further breach 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 with the Data Protection Officer and the SIRO, it will then be referred to the Monitoring Officer for approval and 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 made the breach
- Head of Human Resources or a representative
- Head of ICT/ICT Security Officer
- Head of Media, Marketing and Communications or a representative
- Facilities Management
- 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 breach 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
- 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?
- **Individuals**
  - Notification to the data subjects involved maybe required
- **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.

Appendix 1

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 **Appendix 2**

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 to your AED for action.

Directorate/Service Area	
Assistant Executive Director	
Service Unit Manager/Line Manager	
Employee Reporting Incident	
Person Responsible for Incident	
Date/Time of Incident	
Type of Data*	

* Examples of data:

- Files/Paperwork containing personal data
- Data stored on an information system (e.g. Agresso)
- Emails stored on a laptop/PDA

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. • Health or Social Care? • Financial (e.g. bank details)? • Personally Identifiable Information (e.g. Name, Address, NI Number)? • Sensitive information (e.g. religion, medical)	
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 minimise/mitigate 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**
Telephone: 0161 342 3846 **Email: wendy.poole@tameside.gov.uk**

Appendix 3

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 torecover 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

November 2016

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. Those that are reported will be dealt with in accordance with the procedure outlined below.

1.2 However, disciplinary action may 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 ISI-01 Form has been received it will be passed to Risk Management and Audit who will liaise with Legal Services to evaluate 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 Internal Audit will review the Incident Form ISI-01 in conjunction with Legal Services 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:

- Executive 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 required 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 (referred to in 5.2.4 and 5.2.5) will be conducted in conjunction with HR and will follow the Council's Disciplinary Procedure. At the conclusion of the investigation Internal Audit will issue a report which will be circulated to:

- Executive 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.

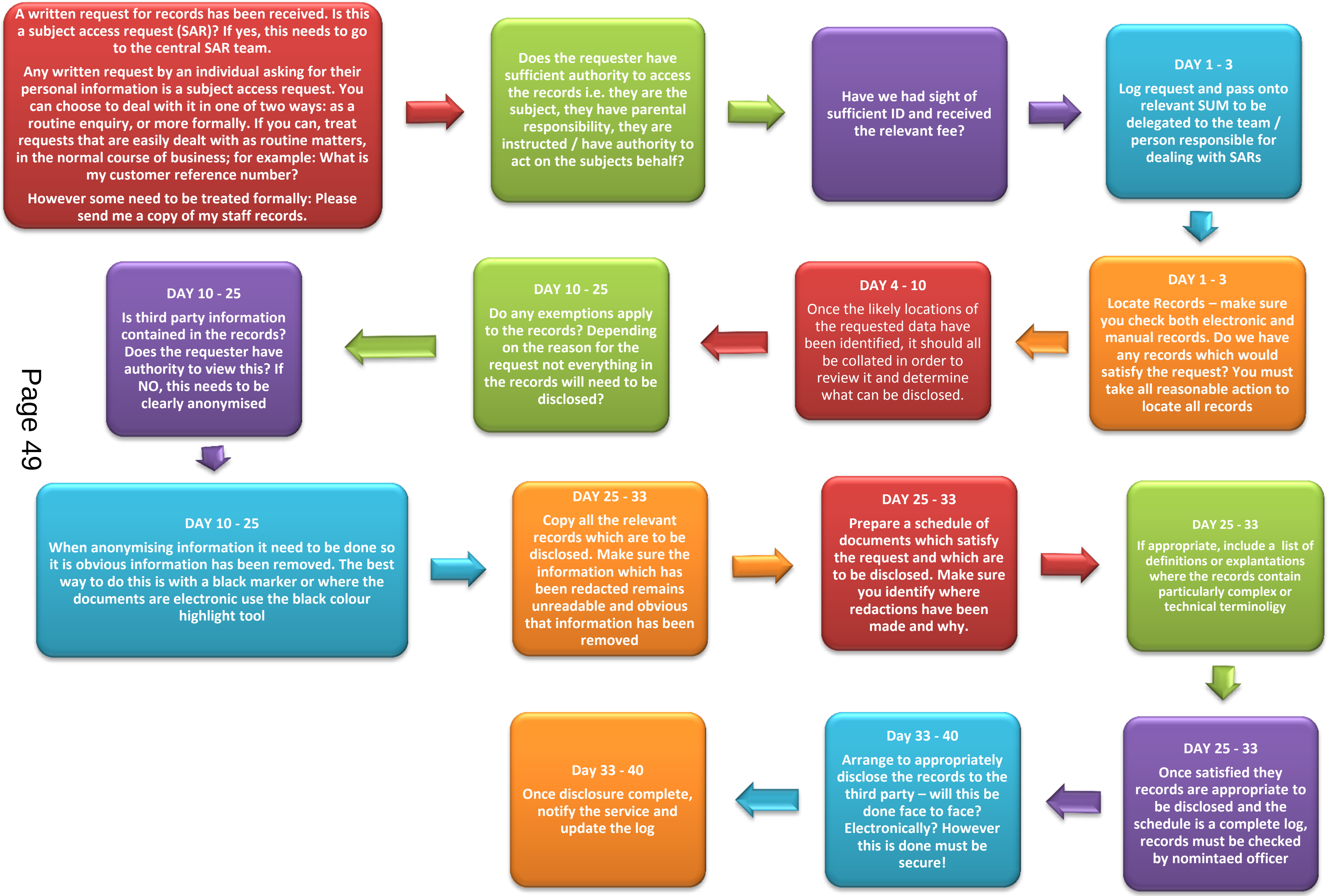
APPENDIX 4

Subject Access Request Guidance

November 2016

CONTENTS

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 - 3

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 - 10

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 10 - 25

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 10 - 25

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 10 - 25

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 25 - 33

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 25 - 33

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 - 33

If appropriate, include a list of definitions or explantations where the records contain particularly complex or technical terminoligy

DAY 25 - 33

Once satisfied they records are appropriate to be disclosed and the schedule is a complete log, records must be checked by nomintaed officer

Day 33 - 40

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 33 - 40

Once disclosure complete, notify the service and update the log

2. INTRODUCTION

2.1 The Data Protection Act 1998 (DPA) gives individuals the right of access to personal information held about them by an organisation. This right is set out in Part 7 of the DPA 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 1998 (DPA). 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**.

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** (executivesuport@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 (0161 342 3859).

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 40 calendar days 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
- Payment of the fee (where requested).

6.2 **Request to be in writing**

A valid SAR must be made in writing, but it does not need to refer to the DPA 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 40 calendar days**.

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

6.9 **Charging a fee**

In most cases, the maximum fee that can be charged by the Council for a SAR is £10. There are exceptions for education and health records, where a fee on a sliding scale up to a maximum of £50 may be charged. **Where the subject making the request is a young person in care etc. the fee is waived**

Payment of a fee is not mandatory, but if a fee is applicable it must be requested from the applicant promptly and in any event within 3 working days.

Upon receipt of a SAR Executive Support must be notified and where a fee is applicable, Executive Support will request and process the relevant fee.

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.

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 40 calendar days 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 4-10**
  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 10-25**
  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 be 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. Template documentation can be accessed here.

- **Quality Assurance – Days 25-33**
  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 33-40**
  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 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 handing 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.

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 it 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.

IDENTIFYING PERSONAL DATA

APPENDIX 1

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

APPENDIX 2

SCHEDULE OF DISCLOSED DOCUMENTS

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		

Agenda Item 5.

Report To: **AUDIT PANEL**

Date: 1 November 2016

Reporting Officer: Ian Duncan – Assistant Executive Director (Finance)

Wendy Poole – Head of Risk Management and Audit Services

Subject: **LOCAL AUDIT AND ACCOUNTABILITY ACT 2014 - CHANGES TO ARRANGEMENTS FOR APPOINTMENT OF EXTERNAL AUDITORS**

Report Summary: This report summarises the changes to the arrangements for appointing External Auditors following the closure of the Audit Commission and the end of the transitional arrangements at the conclusion of the 2017/18 audits.

Recommendations:

1. Members are requested to confirm the preferred option identified in Section 4.

2. Members approve that the Council's Section 151 Officer can take the appropriate actions to progress a commissioning and procurement process, in proposals for the establishment of an Auditor Panel, in consultation with the other Greater Manchester Authorities and the Combined Authority.

Links to Community Strategy: The changes required by the Act will enable the Council to continue to be fully accountable to local people for its financial activities, as part of the Council's commitment to improvement, efficiency and good governance.

Policy Implications: Changes to the terms of reference of the Audit Panel and the establishment of an Independent Auditor Panel will be required.

Financial Implications:

(Authorised by the Section 151 Officer)

Current external fees levels are likely to increase when the current contracts end in 2018.

The cost of establishing a local or joint Auditor Panel outlined in options 1 and 2 below will need to be estimated and included in the Council's budget for 2017/18. This will include the cost of recruiting independent appointees (members), servicing the Panel, running a bidding and tender evaluation process, letting a contract and paying members fees and allowances.

Opting-in to a national Sector Led Body provides maximum opportunity to limit the extent of any increases by entering in to a large scale collective procurement arrangement and would remove the costs of establishing an auditor panel.

Legal Implications:

(Authorised by the Borough Solicitor)

Section 7 of the Local Audit and Accountability Act 2014 requires a relevant authority to appoint a local auditor to audit its accounts for a financial year not later than 31 December in the preceding year. Section 8 governs the procedure for appointment including that the authority must consult and take account of the advice of its auditor panel on the selection and appointment of a local auditor. Section 8 provides that where a relevant authority is a local authority operating executive arrangements, the function of appointing a local auditor to audit its accounts is not the responsibility of an executive of the authority under those arrangements;

Section 12 makes provision for the failure to appoint a local auditor: the authority must immediately inform the Secretary of State, who may direct the authority to appoint the auditor named in the direction or appoint a local auditor on behalf of the authority.

Section 17 gives the Secretary of State the power to make regulations in relation to an 'appointing person' specified by the Secretary of State. This power has been exercised in the Local Audit (Appointing Person) Regulations 2015 (SI 192) and this gives the Secretary of State the ability to enable a Sector Led Body to become the appointing person.

Risk Management:

There is no immediate risk to the Council, however, early consideration by the Council of its preferred approach will enable detailed planning to take place so as to achieve successful transition to the new arrangement in a timely and efficient manner.

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. BACKGROUND TO THE ISSUE

1.1 The Local Audit and Accountability Act 2014 brought to a close the Audit Commission and established transitional arrangements for the appointment of external auditors and the setting of audit fees for all local government and NHS bodies in England. On 5 October 2015, the Secretary of State Communities and Local Government determined that the transitional arrangements for local government bodies would be extended by one year to also include the audit of the accounts for 2017/18.

1.2 The Council's current external auditor is Grant Thornton, this appointment having been made under at a contract let by the Audit Commission. Following closure of the Audit Commission the contract is currently managed by Public Sector Audit Appointments Limited, the transitional body set up by the Local Government Association with delegated authority form the Secretary of State Communities and Local Government. Over recent years we have benefited from reduction in fees in the order of 50% compared with historic levels. This has been the result of a combination of factors including new contracts negotiated nationally with the firms of accountants and savings from closure of the Audit Commission. The Council's current external audit fees are £172,500 per annum.

1.3 When the current transitional arrangements come to an end on 31 March 2018, the Council will be able to move to local appointment of the auditor. There are a number of routes by which this can be achieved, each with varying risks and opportunities. Current fees are based on discounted rates offered by the firms in return for substantial market share. When the contracts were last negotiated nationally by the Audit Commission they covered NHS and local government bodies and offered maximum economies of scale.

1.4 The scope of the audit will still be specified nationally, the National Audit Office is responsible for writing the Code of Audit Practice which all firms appointed to carry out the Council's audit must follow. Not all accounting firms will be eligible to compete for the work, they will need to demonstrate that they have the required skills and experience and be registered with a Registered Supervising Body approved by the Financial Reporting Council. The registration process has not yet commenced and so the number of firms is not known but it is reasonable to expect that the list of eligible firms may include the top 10 or 12 firms in the country, including our current auditor. It is unlikely that small local independent firms will meet the eligibility criteria.

2. OPTIONS FOR LOCAL APPOINTMENT OF EXTERNAL AUDITORS

2.1 There are three broad options open to the Council under the Local Audit and Accountability Act 2014:

Option 1 - To make a stand-alone appointment

2.2 In order to make a stand-alone appointment the Council will need to set up an Auditor Panel. The members of the panel must be wholly or a majority independent members as defined by the Act. Independent members for this purpose are independent appointees, this excludes current and former elected members (or officers) and their close families and friends. This means that elected members will not have a majority input to assessing bids and choosing which firm of accountants to award a contract for the Council's external audit. A new independent auditor panel established by the Council will be responsible for selecting the auditor (assuming there is no existing independent committee such as the Audit Committee that might already be suitably constituted).

2.3 The Chartered Institute of Public Finance and Accountancy has recently published guidance for establishing an Auditor Panel and this is attached at **Appendix 1**.

Advantages/Benefit

2.4 Setting up an auditor panel allows the Council to take maximum advantage of the new local appointment regime and have local input to the decision.

Disadvantages/Risks

2.5 Recruitment and servicing of the Auditor Panel, running the bidding exercise and negotiating the contract is estimated by the Local Government Association to cost in the order of £15,000 plus on going expenses and allowances.

2.6 The Council will not be able to take advantage of reduced fees that may be available through joint or national procurement contracts.

2.7 The assessment of bids and decision on awarding contracts will be taken by independent appointees and not solely by elected members.

Option 2 - Set up a Joint Auditor Panel/local joint procurement arrangements

2.8 The Act enables the Council to join with other authorities to establish a joint auditor panel. Again this will need to be constituted of wholly or a majority of independent appointees (members). Further legal advice will be required on the exact constitution of such a panel having regard to the obligations of each Council under the Act.

2.9 The Joint procurement exercise could involve the ten Greater Manchester Councils and the Greater Manchester Combined Authority.

2.10 At present, eight of the ten Greater Manchester Councils are audited by Grant Thornton and two are audited by KPMG. Given the level of collaboration, joint working and similar core functions across the bodies, there are likely to be benefits from including the ten districts and the combined authority in this procurement. In addition to this, an option could be extended to include health bodies at a later date, although it should be noted that they are currently working to a different timetable for appointments.

Advantages/Benefits

2.11 The costs of setting up the panel, running the bidding exercise and negotiating the contract will be shared across a number of authorities.

2.12 There is greater opportunity for negotiating some economies of scale by being able to offer a larger combined contract value to the firms. It also enables the external auditor to obtain a fuller understanding of the audit requirements across the Greater Manchester level functions.

Disadvantages/Risks

2.13 The decision making body will be further removed from local input, with potentially no input from elected members where a wholly independent auditor panel is used or possible only one elected member representing each Council, depending on the constitution agreed with the other bodies involved.

2.14 The choice of auditor could be complicated where individual Councils have independence issues. An independence issue occurs where the auditor has recently or is currently carrying out work such as consultancy or advisory work for the Council. Where this occurs some auditors may be prevented from being appointed by the terms of their professional standards. There is a risk that if the joint auditor panel choose a firm that is conflicted for this Council then the Council may still need to make a separate appointment with all the attendant costs and loss of economies possible through joint procurement.

Option 3 - Opt-in to a Sector Led Body

2.15 In response to the consultation on the new arrangement the Local Government Association successfully lobbied for Councils to be able to 'opt-in' to a Sector Led Body appointed by the Secretary of State under the Act. A Sector Led Body would have the ability to negotiate contracts with the firms nationally, maximising the opportunities for the most economic and efficient approach to procurement of external audit on behalf of the whole sector.

Advantages/Benefits

2.16 The costs of setting up the appointment arrangements and negotiating fees would be shared across all opt-in authorities.

2.17 By offering large contract values the firms would be able to offer better rates and lower fees than are likely to result from local negotiation.

2.18 Any conflicts at individual authorities would be managed by the Sector Led Body who would have a number of contracted firms to call upon.

2.19 The appointment process would not be ceded to locally appointed independent members. Instead a separate body set up to act in the collective interests of the 'opt-in' authorities. The Local Government Association are considering setting up such a body utilising the knowledge and experience acquired through the setting up of the transitional arrangements.

Disadvantages/Risks

2.20 Individual elected members will have less opportunity for direct involvement in the appointment process other than through the Local Government Association and/or stakeholder representative groups.

2.21 In order for the Sector Led Body to be viable and to be placed in the strongest possible negotiating position the Sector Led Body will need Councils to indicate their intention to opt-in before final contract prices are known.

3. AUDITOR PANEL

3.1 Unless opting into the Sector led body approach (Option 3), there will be a requirement to establish an independent Auditor Panel, either specifically for the Council or in collaboration with partners. The Auditor Panel role is different to that of the Audit Panel. Its functions are to advise the Council on:-

- selection and appointment of the auditor;
- resignation or proposals to remove the auditor;
- adoption of a policy on non-audit services;
- maintenance of independent relationship with the auditor; and
- any proposals to enter into limited liability agreements.

3.2 There is no specific reference in the Act of the Auditor Panel carrying out a contract oversight role but guidance from CIPFA does indicate this is a possible additional function that might be helpful.

3.3 It is anticipated that the Panel will benefit from support specifically from the Head of Paid Service, Treasurer/Section 151 Officer, Head of Internal Audit and Head of Procurement. It also acknowledged that there should be a relationship between the Auditor Panel and the Audit Panel, who will receive updates and assurances arising from the work of the external auditor; and are also well placed to comment on the quality and performance of services provided though the contract. The Act does allow for the Audit Panel to discharge the duties of the Auditor Panel but only if it meets the criteria set out below and that its role when acting as the Auditor Panel is clearly distinct from its role as the Audit Panel.

3.4 A key challenge for the Auditor Panel is to ensure appropriate appointments that meet the requirements of the Act. It is required that the Panel have at least three members but the majority, including the Chair, should be independent of the Council. It is permissible for Council elected members to be represented on the panel, but the majority of members and Chair are required to be independent. The definition of independence in the Act and supporting CIPFA guidance is explicit and allows little option other than through the advertisement and appointment of specific, external, independent members. Auditor Panel members will also be required to have the requisite skills and experience, which may not be readily identifiable or available given the specialist nature of the external audit contract and procurement processes.

3.5 If the Council progresses a single body appointment, it will be required to identify and appoint independent members for this process. The same principle will apply with a joint procurement but the collaborative option means that across the various Greater Manchester level authorities, only one group of independent members would be required and this increases the likelihood of successfully identifying suitably skilled and experienced independent persons to sit on the panel. These are required to be identified through advertisement arrangements and supported by clear panel member role descriptions. The Council and any joint procurement partners will be required to set levels of allowances and expenses.

4. PREFERRED OPTION

4.1 The ten Greater Manchester authorities and the Greater Manchester Combined Authority Treasurers are supportive of the proposal for a Greater Manchester level procurement.

4.2 This option allows for economies of scale, given the 2015/16 combined external audit and grant certification fees of these bodies was approximately £1.8m, whilst also enabling a single firm to be able to discharge external audit functions across Greater Manchester. This will allow the auditor to take a more strategic approach and should facilitate greater added value in supporting the audited bodies on complex accounting and audit matters.

4.3 A joint procurement is also likely to minimise the time and cost of separate procurements across Greater Manchester and will also aid the identification and appointment of an appropriate, effective Auditor Panel, which it is proposed comprises elected members representing the audited bodies as well as a majority of independent members and independent Chair secured following an open process of advertisement and recruitment.

4.4 No costing information is currently available.

5. NEXT STEPS

5.1 The Council has until December 2017 to make an appointment. In practical terms this means one of the options outlined in this report will need to be in place by Spring 2017 in order that the contract negotiation process can be carried out during 2017.

5.2 The Council will need to take action to implement new arrangements for the appointment of external auditors from April 2018. In order that more detailed proposals can be developed and actions progressed the Audit Panel is asked to comment on the options and direct the Council's Section 151 to take forward a preferred option. This will then enable an action plan and detailed proposals to be developed in terms of the procurement approach; composition of the Auditor Panel; scope of audit work and services required; and engagement approach for working across Greater Manchester.

6. RECOMMENDATIONS

6.1 Members are requested to confirm the preferred option identified in Section 4 of the report.

6.2 Members approve that the Council’s Section 151 Officer can take the appropriate actions to progress a commissioning and procurement process, in proposals for the establishment of an Auditor Panel, in consultation with the other Greater Manchester Authorities and the Greater Manchester Combined Authority.

This page is intentionally left blank

Agenda Item 6.

Report To:	**AUDIT PANEL**
Date:	1 November 2016
Reporting Officer:	Ian Duncan – Assistant Executive Director (Finance) Wendy Poole – Head of Risk Management and Audit Services
Subject:	**RISK MANAGEMENT**
Report Summary:	To present to members for comment, challenge and approval the Corporate Risk Register attached at **Appendix 1.**
Recommendations:	That the report is noted and Members approve the Corporate Risk Register at **Appendix 1**.
Links to Community Strategy:	Managing risks will enable the Council to deliver services safely and in an informed manner to achieve the best possible outcomes for residents.
Policy Implications:	Effective 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 risk management 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 and the Code of Corporate Governance.
Risk Management:	Failure to manage risks will impact on service delivery, the achievement of objectives and the Council's Medium Term Financial Strategy.
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 This report presents the revised and updated Corporate Risk Register for comment, challenge and approval.

1.2 Risk Management is facilitated by the Risk Management and Audit Service under the direction of the Head of Risk Management and Audit Services. All risks are owned by the members of the Executive Team, with support from Assistance Executive Directors, managers and staff.

2. CORPORATE RISK REGISTER

2.1 The updated Corporate Risk Register is attached at **Appendix 1**.

2.2 The Senior Management Team have been consulted in compiling the risk register and their comments have been incorporated into the updated risk register.

2.3 The following risks have been merged to remove duplication:-

- **ICT Risk – May 2016**
  The ICT development programme does not keep pace with organisational priorities and challenges facing Council services during the future changes to location and premises. Technical solutions and enhanced performance capacity are not available at the required pace to support major transformational change, budget savings and delivery of business as usual.

- **ICT Risk – May 2016**
  The supporting ICT provision for Council services is not resilient, and does not assure the basic requirements in terms of operational functionality and data security. Major ICT failure or lack of system integrity - Loss of all ICT systems due to an incident which affects the server room/data centre or system failure isolated to a specific system.

- ***ICT Merged Risk – October 2016***
  The supporting ICT provision for Council services is not resilient, it does not keep pace with organisational priorities and change and does not assure the basic requirements in terms of operational functionality and data security. Major ICT failure or lack of system integrity - Loss of all ICT systems due to an incident which affects the server room/data centre or system failure isolated to a specific system.

- **Emergency Planning/BCP Risk – May 2016**
  More frequent extreme weather due to climate change - more frequent occurrences e.g. Flooding, Heat waves, heavy snow and wind damage due to storms.

  Emergency Planning/BCP Risk – May 2016

- Delivery of Services – Failure to provide an appropriate civil contingencies response to an incident or emergency affecting the community or the Council.

- ***Emergency Planning /BCP Risk – October 2016***
  Failure to provide an appropriate Civil Contingencies response to an incident or emergency affecting the community or the Council, including extreme weather conditions due to climate change.

2.4 The following risks have been removed as they have been successfully managed:-

- Collection rates for Council Tax, NNDR and Sundry Debtors are affected by the economic climate.
- Adverse impact on the organisation due to the review of revised Employee Terms and Conditions.

2.5 The following new risks have been added to the register:-

- Failure to manage the local home care market to deliver appropriate and timely care packages.
- Insufficient care home capacity in the local market to provide appropriate placements for people requiring long term care.
- Failure to open a new secondary school in September 2018.

2.6 The Corporate Risk Register will continue to be presented to the Senior Management Team on a quarterly basis and regular updates provided to the Audit Panel. It has also been agreed to separate the risk register into corporate and operational risks recognising that they are different but not of lower or greater weight.

3. SERVICE AREA RISK REGISTERS

3.1 Operational risk registers at Assistant Executive Director Level have been supported by the Senior Management Team and work will now commence to facilitate the production of these registers within service areas during Q3.

3.2 The template used for the Corporate Risk Register will be adopted.

4. RECOMMENDATIONS

4.1 Members note the report.

4.2 Members approve the Corporate Risk Register at **Appendix 1**.

This page is intentionally left blank

Tameside
Metropolitan Borough

APPENDIX 1

Corporate Risk Register - October 2016

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
1	The supporting ICT provision for Council services is not resilient, it does not keep pace with organisational priorities and change and does not assure the basic requirements in terms of operational functionality and data security. Major ICT failure or lack of system integrity - Loss of all ICT systems due to an incident which affects the server room/data centre or system failure isolated to a specific system.	Loss or disruption of services internally and to the community. Loss or corruption of data, which could generate financial implication for reconstitution or additional staff hours to re-establish backups. Whilst systems not functioning fully it provides an opportunity for malicious or criminal abuse of data or systems. Reduction in morale by staff due to inability to carry out role effectively. Reputational damage with the Community as unable to deliver services as required.	Security policy and procedures, physical secure data centre with regular access review, managed, resilient and secure network infrastructure, back up and restore systems, appropriately experienced and qualified technical staff. Funding available to develop DR facility for key council systems, procedures and policies relating to virus infection reviewed and updated to reflect increased risk. The Councils Data Centre is now housed at Rochdale MBC and the partnership arrangements are working well. ICT Strategy being reviewed. Software and hardware being trialled and evaluated for effectiveness of use, so go live procedures work as required. Future planning in place for on going compliance with the PSN requirements. Ability to work without connection to network being reviewed.	**Effective**	5	4	**20**	Robin Monk	Tim Rainey	The provision of ICT is being reviewed as part of the transition to the ICO with the Hospital and the CCG. A Cyber Security Audit is underway in partnership with Salford Computer Audit Services.	Tim Rainey/Nicola Smith/Julie Hayes	Ongoing
2	The demolition of TAC and rebuilding of the service centre does not run to time or budget and the specification is not in line with future service delivery plans.	The identified savings will not be realised. Reputational damage with partners and the Community. Staff and service delivery will be affected.	Updated reports provided to ET, Board and Cabinet. Project Plan/Risk Register in place. External specialist being used to design the new building. Joint Project Board with the College. Internal Project Group chaired by ED - Place.	**Effective**	4	4	**16**	Robin Monk	Damien Bourke			
3 NR	Failure to manage the local home care market to deliver appropriate and timely care packages	Market management is a new requirement of the Care Act. Failure to ensure sufficient supply of good quality home care services could place individuals at risk. There is also a significant impact on the whole health economy if individuals remain in hospital beds because a care package cannot be commissioned. There is financial impact for the economy and reputational risk for the authority.	Tender has been undertaken to bring new providers into the area to improve capacity. TMBC resources are being used to support where there is insufficient capacity to meet need.	Partially Effective	4	4	**16**	Stephanie Butterworth	Sandra Whitehead	Service has been retendered so new providers entering the market. Reablement and homemaker services are covering in emergency situations.		
4 NR	Insufficient care home capacity in the local market to provide appropriate placements for people requiring long term care	Market management is a new requirement of the Care Act. Failure to ensure sufficient supply of good quality care home places could place individuals at risk. There is also a significant impact on the whole health economy if individuals remain in hospital beds because a place at a home of choice is not available. There is financial impact for the economy and reputational risk for the authority.	Discussions are in place with local providers about the level of capacity required in the local economy. At present vacancy level of 7% so manageable, but there is a risk of people not being able to find a bed at their preferred home. Documentation in place at the hospital should an individual and/or their family insist on a specific placement - this may mean moving to an alternative home as an interim arrangement.	Partially Effective	4	4	**16**	Stephanie Butterworth	Sandra Whitehead			

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
5	Failure to deliver council duties to improve the health and wellbeing of Tameside residents.	Poor health outcomes, healthy life expectancy and increasing health inequalities.	Tameside and Glossop Care Together Programme provides a clear strategic commitment to address this risk. Emerging plans and work programmes aim to improve healthy life expectancy and address health inequalities by rebalancing local investments in health and social care. Public Health team members are members/leads in strategic partnerships such as Health and Wellbeing Board, Single Commissioning Management Board. Public Health also have a role in leadership and influencing agendas beyond health and social care commissioning to ensure responsibility for this issue amongst partners and other departments within TMBC is understood, shared and acted upon.	**Effective**	5	3	**15**	Angela Hardman	Debbie Watson/Gideon Smith/Anna Moloney	Annual Public Health business plan and commissioning intentions complying with mandatory guidance. Transition funding secured from GM Health and Social Care Partnership in September 16 for 4 years will support implementation of key elements of Care Together Programme. Model of Care including Healthy Lives and Integrated Neighbourhood Teams agreed.	Debbie Watson/ Gideon Smith/Anna Moloney	2016-20
6	Failing to protect vulnerable children - Vulnerable children are put at risk due to poor systems/processes and reduced service provision.	Service disruption, litigation, loss of public confidence and reputational damage. Negative impact on the service user's life and wellbeing.	Tameside's Safeguarding Children's Board operating effectively. Procedures and guidance in place. Partnership arrangements, information sharing protocols etc. in place. Risk Assessments carried out. Internal and external inspections of services (including schools and private providers) DBS Checks on staff, staff supervision record keeping and training in place. Partnership working with GMP and schools with Project Phoenix (CSE).	**Effective**	5	3	**15**	Stephanie Butterworth	Dominic Tumelty	Changes to further develop teams and provide a cohesive service provision across children's services aim to mitigate risk further, intervene earlier in the life of the problem for a child and have long lasting beneficial impact	Dominic Tumelty	November 2016 Review in April 2017
7	The Council fails to benefit from the opportunities generated from the increased central government devolution to the Greater Manchester Region.	The Council's influence at a regional level is not sufficient for it to maximise the benefits which accrue from devolution such as increased economic growth. Failure to secure funding for the Tameside area including Health Transformational Funding.	The Council is supportive of the current devolution role and is playing a prominent role in shaping the present agreement with Central Government for Greater Manchester. Members and Officers attend meetings of the Combined Authority including the Wider Leadership Team. Lead roles have been allocated to Leaders and Chief Executives to drive the transformation programme forward. The Chief Executive is the lead for Health and Social Care and the Executive Leader leads on investment. With regards to TfGM bids are put in as AGMA collectively so that GM gets it share.	**Effective**	5	3	**15**	Executive Team	Senior Management Team	The Council will deploy adequate resources to ensure that it is able to maximise the benefits.	Senior Management Team	Ongoing
8	The inconsistent application of information standards and controls could result in a significant, unauthorised disclosure of personal and/or sensitive data. Indicating a failure to protect the Council's data and information. With potential for multiple breaches of the Data Protection Act and the Freedom of Information Act	Disruption to service delivery. Reputational damage both regionally and nationally. Financial implications due to compensation claims and costs of putting right damaged caused. Investigation by Information Commissioner, with potential for monetary penalties and enforcement action and the financial impact that goes with these.	Guidance on Intranet. Standard forms introduced. Advice from legal. Publicity, reminders via SMT, corporate screensavers and the Wire. Information Governance Framework developed and implemented. Information Asset Register in place. Information Governance Group in place to keep controls under review. E Tutorials and training and awareness sessions delivered and ongoing support provided. Only encrypted removable devices can be connected to the network and autocomplete of email addresses has been disabled in high risk areas. Email and Files Electronic Retention Policy in place.	**Effective**	4	3	**12**	Sandra Stewart	Aileen Johnson/Tim Rainey/ Wendy Poole	Draft Paperless Policy was considered by SMT in August and is on the agenda for the next Information Governance Group on 28 September. E-Learning courses are being reviewed.	Tim Rainey/Julie Hayes/ Wendy Poole/IGG	November 2016

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
9	Ineffective procurement and contract monitoring - Procurement does not delivery value for money and is not conducted in line with best practice, PSOs and European legislation. The strategic focus on commissioning is less effective due to a lack of skills and capacity to drive the change in culture.	Poor service delivery and increased costs. Legal challenges to contracts awarded would generate financial implications and potential service disruption. Reputational damage amongst suppliers and partners could impact on subsequent tenders and relationships.	Procurement Standing Orders and guidance notes. Training. Internal Audit. Waivers Reports have to be approved by Finance and Legal. Review of Authority spend analysis which highlights suppliers spend over PSO thresholds and aggregate spend for further investigation. Procurement Leads group established. Single Commissioning Function established with TMBC and CCG - new governance - staff currently orienting to the new arrangements.	**Effective**	4	3	**12**	Sandra Stewart and Executive Team	Senior Management Team and Beverley Stephens	The provision of procurement advise and support is currently being reviewed as part of the Resource Management Service Redesign.	Ian Duncan	September/December 2016
10	Impact on service delivery of organisational restructuring and loss of staff. If the workforce continues to decrease in overall numbers there will be reduced opportunities to make appropriate skill matches to meet the changing needs of the organisation. Impacting capacity to deliver statutory or necessary services and service redesigns/transformation is impaired.	Reduction in service quality, along with an impact on morale. Knowledge leakage with loss of experienced staff. Increase in customer complaints. Lack of capacity to deliver service transformation could impact on revenue savings and reform working. Possible reputational damage and impact on the service users and community. Potential for increase in civil claims, e.g. reduced spend on highways could increase the number and cost of compensation claims and increased fraudulent activity. Weak Cost Benefit Analysis models used to support redesign could result in financial issues.	Ongoing structured service redesigns to deliver services within funding envelopes which is monitored by ET. The Big Conversation/Budget consultations with the Tameside Community to help identify how to shape the savings targets around service delivery. GEARS/Annual Development Reviews for staff development. Reports regarding Service Redesigns are presented to Employer Consultation Group (ECG) which ensures the Trade unions are consulted on all changes. ICO looking at different models of service delivery. Partnership working is essential to deliver savings and enable safe services to be delivered going forward.	**Effective**	4	3	**12**	Executive Team	Senior Management Team			
11	The Council is unable to delivery the Medium Term Financial Strategy - Failure to deliver services within reduced budgets and provide for future financial stability.	The corporate savings requirements are not fully understood by the services and the planned service redesigns and savings are not achieved. The full implications of reduced service provision needs to be understood to ensure that a reduction in one area does not cause a cost pressure in another . Staffing cuts, overspends, complaints and reputational damage. Failure to achieve savings targets within timescales will push future years cost pressures up, impacting on future budget reductions.	Budget report presented to Council in February. MTFS updated regularly. Revenue and capital monitoring reported to ET and Board. Recovery plans in place. Service redesigns ongoing to deliver affordable services within funding envelopes. Big Conversation allows the community to help shape the new Tameside. All managers issued with funding envelopes, savings reviewed by ET/SMT, regular budget monitoring and reporting. CDT sessions to ensure managers aware of importance of achieving savings targets. Work is being undertaken by SMT to redesign the shape and size of the council. Agreed corporate projects and priorities. Board Business Day covers the financial savings needed.	**Effective**	4	3	**12**	Sandra Stewart	Ian Duncan	Work is on going with the CCG and Tameside and Glossop Integrated Care NHS Foundation Trust to review the health economy financial position to put plans in place to close the identified gap. Transitional Funding of £23.2m spread over four year has been approved. Different delivery models are being reviewed including a review of support services. Council service budgets are being reviewed and savings identified/challenged to ensure robust delivery plans are in place. Proposed changes to Business Rates need to be monitored and the impact fully evaluated.	Ian Duncan	2016 - 2020
12	Impact of the recession on Tameside - The economic climate affects Tameside to the detriment of residents and local businesses.	Reduced income due to reduction in CT and NNDR payments. Increased potential for fraud. Less grant money available. Increased claims for benefit and debt/housing assistance. Businesses fold and Tameside becomes less attractive to potential investors. Reduced capital receipts.	Significant investment in our Town Centres including Infrastructure improvements, Vision Tameside, assisting local businesses to access funding for investment. Programme of asset disposals drive economic growth. A programme of support for Employment and Skills. Continue to bid for transportation funds. New college building on the old camp street carpark is now open.	**Effective**	4	3	**12**	Robin Monk	Damien Bourke	GM Spatial Framework being developed. Submission, examination and adoption in 2018.	Robin Monk/Damien Bourke	2018

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
13	Ineffective use of data and intelligence to support the decision making process.	Services not fully taking advantage of the information collated by the council to properly inform project appraisals and decision making. Decisions could be challenged if not evidence based. Inefficient and ineffective service delivery to the Community.	Training on Safe and Sound Decisions. Reports reviewed by Legal and Finance to ensure legal and financial implications have been considered fully. Making use of the available insight and intelligence work that the Policy Team coordinate. Information Governance Framework is in place to provide guidance on information use and sharing to ensure the lawful use of Council information and advice can be obtained from Legal and Finance.	**Effective**	4	3	**12**	Sandra Stewart	Wendy Poole/ Sarah Dobson	Information Champions to be established to work with the Information Governance Group to ensure that data is shared across the Council where appropriate to drive process efficiencies.	Wendy Poole	2017
14	Vulnerable adults are put at risk due to poor systems/processes and reduced service provision. Impacting the balance of safeguarding vulnerable people alongside the allocation of Individual Cash Budgets and developing new ways of working to promote independence.	Service disruption, litigations, loss of public confidence and reputational damage. Personal liability of members and / or officers. Negative impact on the service user's life and wellbeing.	Manuals and protocols, Health and Safety training, risk assessments, robust records and systems of inspection, Internal Audit review processes. Full evaluation of changes to service provision undertaken including consultation where appropriate and EIA's. Effective multi-agency Safeguarding Partnership now statutory Board under Care Act legislation.	**Effective**	4	3	**12**	Stephanie Butterworth	Sandra Whitehead			
15	Increased demand for services due to demographic changes - Tameside is unable to meet the needs of its ageing population requiring significant savings to be made, or reductions in levels of dependency, to manage rising levels of demand.	Overspending and overstretching of staff due to increased demand, following cuts in other service areas. Changes to eligibility criteria to 'ration' services may result in reduction of care and support for some, which may have a detrimental effect on health and wellbeing of service users.	Regular review of eligibility criteria, development of prevention strategy to support more people at a lower level of need to prevent dependency on services. Care Together programme, including the development of the ICO is the primary vehicle to develop self-managing and sustaining communities, delivering the right care at the right time to maintain people at home wherever possible.	**Effective**	4	3	**12**	Stephanie Butterworth	Stephanie Butterworth	Development of the Integrated Care Organisation	Sandra Whitehead	April 2017
16	Work on public service reform does not deliver the expected savings and impact on the Community. The internal ability to deliver Public Sector Reform, the savings and transformation agenda is vulnerable to capacity constraints, financial restraints and external policy.	The partners' expectations and performance indicators are not met and could create lack of enthusiasm for working in this way. Potential for reputational damage if the Community does not understand why we are working this way and the benefits to them.	Multi - Agency Communities Teams in place from May 2016. Identification of risk in the community include mental health, ASB and domestic abuse. Key priorities to be addressed to create stronger communities include school readiness, transition into adult hood, worklessness and ageing. Work and progress is reviewed as part of the Strategic Neighbourhood Partnership.	**Effective**	4	3	**12**	Stephanie Butterworth	Emma Varnum	Further integration is planned with the ICO's into 4 Integrated Neighbourhood Teams with Health and Social Care	Emma Varnam	April 2017
17	Impact on the Council in relation to the changing landscape for schools including; Free Schools, Academisation and linked issues relating to BSF/PFI.	Loss of Land. Reputational damage for the Council if Free Schools/Academies do not perform to acceptable standards. Potential financial impact on the council if schools transfer to an academy with a deficit in place. Funding/legal implications for BSF/PFI schools. Impact on support services within the Council.	Deficit recovery planning support in place. The Council is only liable for a deficit if it instigates the associated Academy conversion. . Support services to schools will be reviewed during 2016/17. A clear strategy is in place to support schools which is regularly monitored by the Council's Education Attainment Improvement Board.	**Effective**	4	3	**12**	Sandra Stewart/ Robin Monk/ Stephanie Butterworth	Damien Bourke/ Bob Berry/ Ian Duncan	Review of support services to schools to be undertaken, new arrangements to be implemented by April 2017. Local Partnerships are undertaking a review of the PFI contracts currently in place to determine the opportunities to reduce cost and ensure affordability over the contract duration	**Support Services** Ian Duncan/ Tracy Brennand **PFI/BSF** Robin Monk	**Support Services** April 2017 **PFI/BSF** December 2016
18	Requirements of the Care Act on service provision and associated financial implications.	Additional demands on assessed care provision and associated additional cost.	Ongoing review of Adult Social Care service delivery alongside Care Act requirements. This includes reduced dependency on residential care and increased independent living at home at lower cost.	**Effective**	4	3	**12**	Stephanie Butterworth	Sandra Whitehead			

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
19	Failure to provide an appropriate Civil Contingencies response to an incident or emergency affecting the community or the Council, including extreme weather conditions due to climate change.	Loss of accommodation, key staff, IT services, records/information, equipment. Unable to supply the legally required and identified emergency level of service to customers and service users. Loss of reputation regionally and nationally. Care in the Community overstretched and potential impacts on other front facing services depending on the nature of the incident. Public fear and concern along with potential accommodation problems. Service failure. Drains and sewers unable to cope with volume of rainfall. Community safety implications with heat stroke. Increase potential for Infrastructure and property damage, with fires, settlement and storm damage. Reputational impact. Possibility of an increase in the number of insurance claims. Accommodation problems. Public concern.	Corporate Business Continuity Pans in place supported by Directorate BCP's, Executive/IMT Plan. Subsequent development is underway to review BC process, delivery and planning. Emergency Plan, Community Risk Register, Statutory Duties. Director on Call in place and a Forward Incident Officer. Regular meetings and forums with Blue Light services and other LAs. Central GM Civil contingencies Team in place. Plans are tested. Flood plan in place.	**Effective**	5	2	**10**	Robin Monk/ Sandra Stewart	Ian Saxon/ Wendy Poole	Business Continuity system is under review to meet with the needs of the Council.	Wendy Poole	December 2016
20	Failure to support schools effectively to achieve a judgement of good/outstanding by Ofsted	If schools are unable to make the level of progress required to assure Ofsted that all children are receiving a good standard of education, the Council could attract a full inspection of its school Improvement Support Services by Ofsted. A worst case scenario would result in this function being removed from the Council. The reputational damage to the Council would be very significant.	The Council has invested in the creation of a new School Performance and Standards Team as well as adding capacity in other areas of the education service which all support the school improvement agenda. A clear strategy is in place to support schools which is regularly monitored by the Council's Education Attainment Improvement Board. Currently - September 2016 - 93% of primary age pupils attend a Good or better primary school, but the proportion for secondary age students is only 53%.	Effective	5	2	**10**	Stephanie Butterworth	Bob Berry			
21	The property portfolio rationalisation necessary for the delivery of appropriate council wide services is not delivered and consequently savings are not achieved.	The Council will have an unnecessary financial burden in respect of unoccupied or under used properties. Impact on the overall funds for the Council and compliance with the MTFS.	Programme of asset disposals by value. Regular sales at auction. Progressing major sites to outline planning. There is a strategy in place which is considered by the Strategic Planning and Capital Monitoring Group, and disposals are approved by Cabinet. There is a process in place to delivery £55m over 3 years. Sites/buildings to go to the Market are discussed monthly with the Executive Member.	**Effective**	3	3	**9**	Robin Monk	Damien Bourke	Capital Officer Working Group being set up by Finance.	Ian Duncan	September 2016
22 NR	Failure to open a new secondary school in September 2018.	The borough will have failed to provide sufficient school places for approximately 300 young people. Reputational damage.	Detailed pupil planning projections from officers indicate a 'bulge' year for secondary places in 2018. This data also indicates the geographical location of where projected gaps in provision are.	Effective	3	3	**9**	Stephanie Butterworth	Bob Berry	Planning is under way with EFA, RSC, Laurus Trust, and council officers.	Bob Berry/ Damien Bourke	Sept. 2018
23	Insurance purchased inappropriate or inadequate to provide necessary cover for the Council's risks.	Increased costs, service interruption, potential litigation/fines complaints and reputational damage. Financial impact due to the uninsured claims having to be settled with none budgeted funds.	Annual Renewal Process undertaken in conjunction with Insurance Brokers (AON). Insurance contract let every 5/7 years in conjunction with our Insurance Brokers. Regular review meetings take place with Brokers/Insurers/Claims Handlers to monitor performance and to discuss changes in the insurance market and keep abreast of new claim trends and discuss any litigation issues or court rulings that could have impact. Members of the North West Insurance Officers Group.	**Effective**	4	2	**8**	Sandra Stewart	Wendy Poole	Introducing quarterly review meetings with Resource Management to insurance matters. Annual Insurance Report to be presented to SMT. The procurement of Cyber Insurance will be re-assessed as part of the 2017 /18 renewal process taking on board the Audit findings referred to in risk 1.	Wendy Poole	October 2016 Annually thereafter for SMT Report

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
24	Pension Fund investments do not provide the appropriate/anticipated level of return/ income, to support the development of the fund.	Increased employer costs. Reputational damage to the Fund and overall stakeholder concern.	Investments are placed with different fund managers diversified across different asset classes and countries. Markets are monitored daily with the Fund's performance being a major item at each quarterly meeting of the Pension Fund Management Panel. The Funds operations are subject to both internal and external audit. There is also a statutory valuation of the Fund every three years, part of which is to compare assets to liabilities.	**Effective**	4	2	**8**	Sandra Stewart	Steven Taylor/Paddy Dowdall			
25	Inability to appropriately store and retrieve digital records and media in a future proof format.	Loss of data. Unable to retrieve digital records. Staff encouraged to use centralised storage and not removable drives. Financial implications with the cost of paper storage increasing. Financial and time implications of reconstructing data/information. Potential for litigation or fines from the ICO.	IT Back-Up system in place. Daily and weekly back ups taken. Back ups are stored off site. The Data Centre is now located in Rochdale MBC's 'Server room located at 1 Waterside Rochdale. Horizon scanning for future developments and improvements. Information Governance Framework in place, all staff should be reviewing the files they have in line with the Retention and Disposal Guidance. Information Asset Registers in place. Retention Policy for emails/files in place and project to put in place EDRMS and case management for all services underway.	**Effective**	4	2	**8**	Robin Monk	Tim Rainey/Julie Hayes	Draft Paperless Policy was considered by SMT in August and is on the agenda for the next Information Governance Group on 28 September.	Tim Rainey/Julie Hayes	Ongoing
26	Alignment of partnership working - Inability to ensure that partnership arrangements deliver agreed outcomes. Increased pressures and reduced capacity on external providers to develop and provide services.	Failure to deliver planned outcomes, loss of credibility and reputational damage. Damage to morale, financial and resource implications. Possible litigation. Partners not being in the same place as the Council. Reduced market capacity and choice of consumers.	Corporate Plan is monitored regularly by Executive Team and Board. The governance arrangements regarding the ICO are now in place and decisions are made by a Joint Commissioning Board and the Executive Cabinet depending on the nature of the decision.	**Effective**	4	2	**8**	Executive Team	Senior Management Team			
27	Failure to target resources at the right families with the right intervention across early years and worklessness settings.	Financial and reputational implication of work and contacts. Improvements not achieved in accordance with the government funded scheme.	Early Years is a key strategic priority, including new commissioning responsibilities for HV/FNP. Worklessness a key strategic priority for new Communities teams in operation from May 16.	**Effective**	4	2	**8**	Stephanie Butterworth	Dominic Tumelty/Emma Varnum/Emma Handby			
28	Local Government Pension Scheme asset pooling requirements not met.	Government uses its powers to direct the Fund as set out in the new Investment Regulations. Reputational damage to the Fund and overall stakeholder concern.	Fund has chosen pooling partners and submitted a response to Government. Professional advice will be sought throughout process.	**Effective**	4	2	**8**	Sandra Stewart	Euan Miller	Awaiting feedback on proposals submitted in July 2016. Feedback received will inform future actions. Successful pooling outcomes will result in improved net investment returns and lower employer contribution rates.	Euan Miller	October 2016
29	Failure to reconcile Guaranteed Minimum Pension (GMP) data prior to the HMRC notifying citizens in 2018 of their accrued GMPs and the authorities responsible for them.	A great deal of failure demand and loss of reputation. Incorrect amounts of pensions may be paid.	An overview project plan has been drawn up and the project is being monitored by the Fund's Management Team at their regular meetings. Some initial work has already been undertaken and meetings with two companies are scheduled.	**Effective**	4	2	**8**	Sandra Stewart	Emma Mayall	Quotes are to be sought during Q3 regarding having the GMPF/HMRC data surveyed to assess the scale of the work that is going to be involved.	Emma Mayall	December 2016

	Risk Description	Description of Impact	Controls in Place to Mitigate Risk	Evaluation of Controls	Impact score	Likelihood score	Risk Rating (Impact x Likelihood)	Risk Owner (Executive Director)	Responsible AED/SUM	Proposed Actions - include resulting benefit and costs	Responsible Officer	Target Date for Proposed Action
30	Failure to prevent or detect acts of significant fraud or corruption with consequent financial or reputational damage to the Council.	Financial loss to the Council and reputational damage. Adverse publicity both locally and nationally. Investigations are resource intensive. Prosecutions can tale a long time to conclude.	Fraud risk assessment carried out by Internal Audit. Internal Audit review systems on a cyclical basis to provide assurance that effective controls are in place and working. Internal Audit provide advice and support to managers to ensure the control environment is considered when changes are being proposed. Anti Fraud, Bribery and Corruption - Statement of Intent in place. Fraud Response plan in place. Whistleblowing Policy in place. Management are responsible for the control environment and this is tested as part of the Annual Governance Statement process as Executive Directors sign assurance letters. All ongoing investigations are reported to the Standards Panel and summary data is presented to the Audit Panel as part of regular progress reports by the Head of Risk Management and Audit Services.	**Effective**	3	2	**6**	Sandra Stewart	Ian Duncan/ Wendy Poole	Investigation process and fraud documents are being reviewed to ensure they adhere to best practice.	Wendy Poole	December 2016
31	In-effective community cohesion. The community cohesion activities undertaken do not have the required results, of raising awareness, integration and acceptance within the community.	Unrest, riots and vandalism. Inequalities within the community becoming more prevalent and raising community tension. Potential to lead to an increase in crime and disorder. Failure to comply with Equality Legislation could lead to reputational damage and litigation.	A well established Strategic Neighbourhood Partnership and sub groups are established. With regular tension and performance monitoring through THIP group, plus Prevent and Channel Groups. An action plan to improve cohesion has been written and is being enacted. A high level intervention group has been identified for when tensions arise, threat analysis forms part of service planning.	**Effective**	3	2	**6**	Stephanie Butterworth	Emma Varnam	Community Safety structure is being reviewed to ensure an appropriate strategic oversight.	Emma Varnam	Ongoing

This page is intentionally left blank