

Public Document Pack



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

AUDIT PANEL

Day: Tuesday
Date: 12 March 2024
Time: 2.00 pm
Place: Committee Room 1 - Tameside One

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 1 February 2024 to be signed by the Chair as a correct record.	1 - 8
4.	2022-23 AUDIT STRATEGY MEMORANDUM (ASM) To receive a report of the First Deputy (Finance, Resources and Transformation) / Director of Resources.	9 - 42
5.	EXTERNAL AUDIT PROGRESS REPORT To receive a report of the First Deputy (Finance, Resources and Transformation) / Director of Resources.	43 - 56
6.	ANNUAL GOVERNANCE STATEMENT ACTIONS FOLLOW UP To receive a report of the Head of Assurance.	57 - 64
7.	INFORMATION GOVERNANCE POLICIES To receive a report of the Head of Assurance.	65 - 106
8.	INTERNAL AUDIT PLAN, CHARTER AND QUALITY ASSURANCE & IMPROVEMENT PROGRAMME To receive a report of the Head of Assurance.	107 - 136
9.	AUDIT PANEL WORK PROGRAMME 2023/24 To receive a report of the Head of Assurance.	137 - 140
10.	STATEMENT OF LOCAL AUTHORITY CLAIMED ENTITLEMENT TO HOUSING BENEFIT SUBSIDY FOR FINANCIAL YEAR 2022/2023 To receive a report of the Assistant Director, Exchequer Services.	141 - 158

From: Democratic Services Unit – any further information may be obtained from the reporting officer or from Natasha Matthews, Senior Democratic Services Officer, to whom any apologies for absence should be notified.

Item No.	AGENDA	Page No
11.	STAR PROCUREMENT UPDATE To consider a report from the Assistant Director of STAR Procurement.	159 - 166
12.	URGENT ITEMS To consider any additional items the Chair is of the opinion shall be dealt with as a matter of urgency.	
13.	DATE OF NEXT MEETING To be confirmed.	

From: Democratic Services Unit – any further information may be obtained from the reporting officer or from Natasha Matthews, Senior Democratic Services Officer, to whom any apologies for absence should be notified.

Agenda Item 3.

AUDIT PANEL

1 February 2024

Commenced: 14:00

Terminated: 14:50

Present: Councillors Fitzpatrick (Chair), Boyle, Bray, Kitchen, McLaren and Smith
Ian Duncan (Independent Member)

In Attendance:

Sandra Stewart	Chief Executive
Ashley Hughes	Director of Resources
Paddy Dowdall	Assistant Director, Local Investment and Property
Gemma McNamara	Interim Assistant Director, Finance
Carol McDonnell	Head of Assurance
Thomas Austin	Senior Finance Manager
Stuart Munro	Finance Manager
Karen Murray	Mazars
Amelia Salford	Mazars
Martin Nixon	Risk, Insurance and Information Governance Manager

Apologies for Absence: Councillor Billington and Stuart Fair (Independent Member)

28. DECLARATIONS OF INTEREST

There was no declarations of interest.

29. MINUTES

The minutes of the Audit Panel meeting on the 21 November 2023 were approved as a correct record subject to the following amendment:

Minute 24 which read as:

RESOLVED

That the Audit Panel discuss and agree the proposed draft annual self - assessment checklist and any actions required to improve effectiveness.

Being amended to:

That the Audit Panel agreed the proposed draft annual self - assessment checklist and any actions required to improve effectiveness.

30. TAMESIDE AUDIT COMPLETION REPORT 2021/22 (ACR)

Consideration was given to a report of the external auditors Mazars, summarising the approach, planning and findings related to the audit of the 2021/22 Statement of Accounts. The 2021/22 Audit Completion Report was issued as part of the completion of the external audit.

Members were advised that Mazars had substantially completed their audit in respect of the financial statements for the year ended 31 March 2022. An Audit Completion Report 2021/22 for TMBC was attached at appendix 1 and Members were further provided with an updated Audit Completion Report which included updated management responses.

With regards to significant findings, Mazars reported that their work on management override of controls and valuation of surplus assets was completed and Members were pleased to hear that there was no matters to be brought to the Panel's attention.

As reported previously, Mazars explained that the Council's accounts contained material balances and disclosures relating to its holding of property, plant and equipment ("PPE") including investment properties, with the majority of property assets required to be carried at valuation. Mazars identified errors in the inputs used in the valuer's calculations and it was explained that the work carried out by Mazars' valuation team identified differences between the land values used by the valuer and available comparable data. It was explained that the land values for 2021/22 and 2022/23 had been reviewed by both finance and estate teams, and challenged where appropriate based on unusual or unexpected movements, or where contradictory to other market data such as sales prices available to estates. Mazars reported that through audit testing of valuations in 2021/22, there were no issues identified with land values and therefore Mazars advised that they were satisfied that this recommendation was appropriately implemented by management.

Mazars informed the Panel the new Section 151 Officer (February 2022) was working closely with Mazars to understand the improvements required going forward and was supportive in driving the 2021/22 audit forward in order to be back on track with the delivery of audit on time. In regards to the Value for Money Conclusion, the Section 151 Officer assured Members that the Council's Value for Money self-assessment was completed and would be circulated to Mazars as soon as possible. Members were advised that Mazars' would complete their final review of the statements upon receipt of the signed version of the accounts and letter of representation.

Detailed discussion ensued with regards to the report and the outstanding matters included within the report. Members discussed the various audit areas including PPE and the impact of RAAC on the asset portfolio. Discussion ensued in respect of this and it was explained that further information from surveyors would be provided to Mazars.

RESOLVED

- (i) To note the content of the 2021/22 Audit Completion Report at Appendix 1; and**
- (ii) To approve the updated Annual Governance Statement at Appendix 2 following the conclusion of the 2021/22 audit.**

31. GMPF AUDIT COMPLETION REPORT 2022/23 (ACR)

Consideration was given to a report of the external auditors Mazars, highlighting the key matters arising from the 2022/23 financial statements for the Greater Manchester Pension Fund (GMPF).

An Audit Completion Report for the Greater Manchester Pension Fund for year ended 31 March 2023 was attached at Appendix 2. Mazars reported that they had substantially completed their audit in respect of the financial statements for the year ended 31 March 2023 and there were no matters which Mazars were aware of, that required modification of their audit opinion. Mazars further expressed their thanks to GMPF officers for their co-operation during the course of the audit.

Members of the Panel were advised that GMPF's statement of accounts formed part of the financial statements for Tameside Council, as the administering authority of the Fund. This meant they were unable to provide their opinion on the Fund's accounts until Mazars had completed their audit for the administering authority.

Mazars advised the Panel with regard to internal control recommendations and summarised their findings in relation to audit misstatements which included unadjusted misstatements totalling £70m. As reported previously, the unadjusted item was the estimation of a potential error in the valuation of level 3 investments. Mazars explained that their estimate was driven by known differences identified in a sample of investments selected for detailed testing. The differences within the sample arose due to a timing difference between information used by the Fund to prepare accounts and be information available at the time of sample testing. However, Members were advised that this was below the materiality threshold and therefore GMPF had not adjusted for this misstatement based on immateriality.

RESOLVED

That the report be noted.

32. STATEMENT OF ACCOUNTS 2021/22

Consideration was given to a report of the First Deputy (Finance, Resources & Transformation) / Director of Resources. The report presented the Statement of Accounts for Tameside MCB and the Greater Manchester Pension Fund for year ended 31 March following completion of the External Audit.

It was explained that the Statement of Accounts 2021/22 provided full details of the Council's financial position at 31 March 2022 and its income and expenditure for the year there ended. The accounts were prepared in accordance with the CIPFA Code of Practice for Local Authority Accounting, which was based on International Financial Reporting Standards. The full financial statements, including the statements for the GMPF, were included at Appendix 1.

As considered earlier on the agenda in the Audit Completion Report, details of the misstatements and the impact on different elements of the financial statements were discussed. The Director of Resources summarised the main misstatements to the Panel, which included unadjusted and adjusted misstatements.

It was explained that a number of other presentational amendments had been made to the Statement of Accounts which improved the presentation and disclosure of financial information requirements of the CIPFA Code of Practice. The presentational adjustments recommended by external audit had also helped to improve the overall quality of accounts and had not impacted on the financial position reported.

Members were advised that the external audit of the Statement of Accounts was substantially completed but subject to final review, conclusion of the Value for Money Assessment and completion procedures by External Audit. The Director of Resources advised that the Value of Money assessment was ready to go subject to final review.

RESOLVED

That the Audit Panel are asked to:

- 1. Note the findings of external audit reported in the previous agenda item and summarised in section 3 below;**
- 2. Approve the Statement of Accounts for 2021/22, subject to the conclusion of the external audit, noting the ongoing work on Value for Money; and**
- 3. Approve delegated authority to the Director of Resources to agree any further presentational amendments to the financial statements arising from the conclusion of the external audit. In the unlikely event of any substantive amendments to the primary statements, these will be discussed with the Chair of Audit Panel prior to the signing and publication of the final audited Statement of Accounts.**

33. TREASURY MANAGEMENT STRATEGY 2024/25

Consideration was given to a report of the Director of Resources. The report detailed the Treasury Management Strategy for 2024/25.

The Panel were advised that the Treasury Management service was an important part of the overall financial management of the Council's affairs. At 31 December 2023 the Council had £121m of investments which needed to be safeguarded and £139m of long term debt, which had been accrued over the years to help to fund the Council's capital investment programmes. The significant size of these amounts required careful management to ensure that the Council met its balanced budget requirement under the Local Government Finance Act 1992. Generating good value for money was

therefore essential, in terms of both minimising the cost of borrowing and maximising the return on investments.

It was explained that the Council's current strategy was to maintain borrowing and investments below their underlying levels, known as internal borrowing. The strategy of internal borrowing was beneficial as the interest charged on borrowing was greater than that available on investments, and also had the benefit of reduction to the Council's exposure to counterparty credit risk. It was reported that it was not anticipated that any further borrowing would be taken up in the short term.

Under the Local Government Act 2003, the Department for Communities and Local Government issued in March 2010 revised "Guidance on Local Government Investments". The 2003 Act requires an authority "to have regard" to this guidance. Part of this guidance was that "A local authority shall, before the start of each financial year, draw up an Annual Investment Strategy for the following financial year, which could vary at any time. The strategy and any variations were to be approved by the full Council and were to be made available to the public." This strategy was provided to Members of the Panel at Appendix 1.

RESOLVED

That the Treasury Management Strategy for 2024/25 be noted.

34. CAPITAL STRATEGY 2024/25

Consideration was given to a report of the Director of Resources, which detailed the Capital Strategy for 2024/25.

It was explained that the CIPFA Prudential Code (revised 2021) required that the Council produced an annual Capital Strategy. The Strategy was the Council's framework for the allocation and management of capital resources within the authority, which took into account the Council's key priorities in the Corporate Plan. This formed a key part of the Council's integrated revenue, capital and balance sheet planning with a view towards deliverability, affordability, sustainability and risk.

It was reported that the Council maintained a three year Capital Programme, which covered the periods 2023/24 to 2025/26. This was updated annually during the budget process in February and quarterly during the year. As at December 2023, the Programme had a total value of £116m, which included both fully approved and earmarked schemes. Members were provided with a summary of the Programme at Appendix 1A of the report.

Members were provided with the main objectives of the Council's Capital Strategy and how this linked to the Council's Corporate Plan, "Our People, Our Place, Our Plan". It was explained that the Strategy demonstrated that the Council continued to work closely with a variety of partners to obtain quality projects and maximise potential resources in the achievement of its aims. The Council further encouraged the continued exploration of securing external funding, the examination of different forms of procurement and maintaining current levels of innovation.

Members were further informed that the Council had a good framework in place to achieve its strategy and would strive to achieve continual improvement on a number of its planning processes within the main objectives. Members were assured that this would be monitored and reviewed by the Strategic Planning and Capital Monitoring Panel.

RESOLVED

That the Capital Strategy for 2024/25 is approved.

35. STRATEGIC RISK MANAGEMENT UPDATE (QUARTER 3)

Consideration was given to a report of the Head of Assurance / Risk, Insurance and Information

Governance Manager, which presented the Council's strategic risk management update (quarter three).

As reported at the last Audit Panel meeting, members were advised that the 'three lines' had been introduced as part of a number of enhancements to the Council's risk management arrangements as part of the Council's wider embedding of the assurance model.

The Head of Assurance summarised the various updates on the improvements set out in the action plan at the last Audit Panel. In relation to Directorate Risk Registers, it was reported that each Directorate had commenced the process and compiled their Risk Registers to include the '3 lines' and Members were advised that good progress had been made in relation to this.

It was explained that the strategic risk register had been updated for Quarter 3 (January 2024) and this was provided to Members at Appendix 1 which included updated comments.

RESOLVED

That the report be noted.

36. INTERNAL AUDIT PROGRESS REPORT – DECEMBER 2023

Consideration was given to a report of the Head of Assurance which provided an update on Internal Audit's progress against the Internal Audit Plan as at 31 December 2023.

As advised at previous meetings, it was explained that progress had been slower than anticipated due to resourcing issues. The Head of Assurance reported that much of the early part of the year was spent finalising 2022/23 reports and providing the annual opinion and draft plan.

Members were provided with the 2022/23 reports that were completed in 2023/24 at appendix 1 of the report. It was reported that progress was made on the recruitment of an Interim Audit Manager whilst a Service Review was completed. The contract with SWAP was in progress flexed to provide additional work to be completed as soon as possible.

The summary of progress against the 2023/24 plan was detailed at Appendix 2. Members were provided with the overall assurance rating and audit findings, together with recommendations for action and management responses which were set out within Internal Audit's reports.

Members were advised that the Council was committed to providing effective counter fraud arrangements and ensured that there were adequate measures in place which prevented, detected and investigated fraud corruption. It was reported that internal audit had two counter fraud specialists who facilitated the co-ordination of the GMPF's counter fraud activities. A summary of the work undertaken on unplanned / irregularity / fraud referrals during the period was detailed at Appendix 3.

It was explained that no specific issues had been highlighted through the work undertaken by Internal Audit during this period. A reduction in the number of open recommendations was evident and the Head of Assurance summarised the current figures for outstanding recommendations that had passed their due date for implementation.

As previously reported to the Panel, a root and branch review of audit practice was undertaken as part of the implementation of the assurance model and this progress was reported to the Panel in November 2023. A review of the assurance ratings had commenced since the permanent Head of Assurance commenced in post. The proposed priority and assurance ratings were provided to Members at Appendix 8 and this was to be adopted from the next financial year.

Members were advised that to ensure the quality of the work performed, Internal Audit had a programme of quality measures which included:

- Supervision of staff who conducted audit work;

- Review of files of working papers and reports by managers;
- Regular networking with professional / technical bodies and peers.

Detailed discussion ensued in relation to the report and the Head of Assurance confirmed that risk-based arrangements regarding Adult Social Care were no longer on hold. Members further felt compliance on findings and recommendations should be implemented by the relevant officers as soon as possible.

RESOLVED

That the Audit Panel note the progress report at Appendix 1.

37. COUNTER FRAUD APPROACH AND UPDATE

Consideration was given to a report of the Head of Assurance. The report presented the refreshed Counter Fraud Approach which included a Counter Fraud Policy, Strategy and Action Plan. Members of the Audit Panel were further provided with a counter fraud update, refreshed Anti-Money Laundering Policy and the new Prevention of Tax Evasions Policy.

Members were advised that the Council's Counter Fraud approach was in need of review and had undergone a major refresh in order to ensure that it was fit for purpose. The new Counter Fraud approach included a refreshed Policy and Strategy, together with an Action Plan, which had been drafted with the aim to tackle the threat from fraud, bribery and corruption.

It was explained that the new approach considered the Fighting Fraud & Corruption Locally (FFCL) Strategy for the 2020's, which was aimed at council leaders, chief executives, financial directors and all those charged with governance in local authorities including those on audit committees and with portfolio responsibility. The Strategy included the Five Pillars Framework which showed the vital components of an effective and proactive response to the risks:

- Govern;
- Acknowledge;
- Prevent;
- Pursue;
- Protect.

The Counter Fraud Strategy was accompanied by a Counter Fraud Action Plan and the aim of the action plan was to set out high level actions for the Assurance function to embed the new Strategy. The high level action plan was supported by an operational plan which aimed to deliver the new approach, and these actions were subject to regular review and monitoring by the Head of Assurance.

Members were provided with analysis of the movement and 2023/24 activity in cases for the last three months. Of the 74 cases dealt with this year, it was reported that 49 were investigations with the remaining 25 being cases that related to services that required assistance. Members were advised that there were 20 open cases and a breakdown of open cases for the last four months by fraud type was provided within the report.

RESOLVED

That the Audit Panel approve the report.

38. AUDIT PANEL WORK PROGRAMME 2023/24

Consideration was given to a report of the Head of Assurance which detailed the Audit Panel's Work Programme for 2023/24.

To assist the Audit Panel with delivering its terms of reference, officers had prepared the updated

work plan for 2023/24, which set out the areas that should be considered by the Audit Panel. The work plan provided at Appendix 1 listed the items that Audit Panel would discuss for 2023/24.

Discussion ensued in relation to the report and highlighted the benefits that a private meeting with the Internal and External Auditors provided for good practice.

RESOLVED

That the report is noted.

39. URGENT ITEMS

There were no urgent items for consideration.

40. DATE OF NEXT MEETING


That the next meeting of the Audit Panel was scheduled to take place on 12 March 2024, be noted.

CHAIR

This page is intentionally left blank

Agenda Item 4.

Report to:	AUDIT PANEL
Date:	12 March 2024
Executive Member/ Reporting Officer:	Cllr Jacqueline North – First Deputy (Finance, Resources & Transformation) Ashley Hughes – Director of Resources
Subject:	2022-23 AUDIT STRATEGY MEMORANDUM (ASM)
Report Summary:	The 2022-23 Audit Strategy Memorandum is a high level planning document by the Council’s external auditors, setting out work processes and timetables to complete the audit of the 2022-23 accounts.
Recommendations:	To note the content of the 2022-23 Audit Strategy Memorandum.
Corporate Plan:	The report supports the Council’s Corporate Plan objectives.
Policy Implications:	There are no direct policy implications flowing from the Statement of Accounts.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	An audited statement of accounts gives assurance on the Council’s finances.
Legal Implications: (Authorised by the Borough Solicitor)	The requirement to externally audit the Council’s statement of accounts is set out in the Accounts and Audit (England) Regulations 2015.
Risk Management:	The external audit provides verification of the financial statements.
Access to Information:	The report is to be considered in public.
Background Information:	The background papers relating to this report can be inspected by contacting Stuart Munro, Senior Finance Manager.

 Telephone: 0161 342 4257

 e-mail: stuart.munro@tameside.gov.uk

This page is intentionally left blank

Audit Strategy Memorandum

Tameside Metropolitan Borough Council

Year ending 31 March 2023

Page 11



Contents

01 Engagement and responsibilities summary

02 Your audit engagement team

03 Audit scope, approach and timeline

04 Significant risks and other key judgement areas

05 Value for money

06 Fees for audit and other services

07 Our commitment to independence

08 Materiality and misstatements

A Appendix A – Key communication points

Appendix B – Revised auditing standard on Identifying and assessing the risks of material misstatement: ISA (UK) 315 (Revised 2019)

Page
12

This document is to be regarded as confidential to Tameside Metropolitan Borough Council. It has been prepared for the sole use of the Audit Panel as the appropriate sub-committee charged with governance. No responsibility is accepted to any other person in respect of the whole or part of its contents. Our written consent must first be obtained before this document, or any part of it, is disclosed to a third party.

12 March 2024

Dear Members of the Audit Panel

Audit Strategy Memorandum – Year ending 31 March 2023

We are pleased to present our Audit Strategy Memorandum for Tameside Metropolitan Borough Council for the year ending 31 March 2023. The purpose of this document is to summarise our audit approach, highlight significant audit risks and areas of key judgements and provide you with the details of our audit team. As it is a fundamental requirement that an auditor is, and is seen to be, independent of its clients, section 7 of this document also summarises our considerations and conclusions on our independence as auditors. We consider two-way communication with you to be key to a successful audit and important in:

- reaching a mutual understanding of the scope of the audit and the responsibilities of each of us;
- sharing information to assist each of us to fulfil our respective responsibilities;
- providing you with constructive observations arising from the audit process; and
- ensuring that we, as external auditors, gain an understanding of your attitude and views in respect of the internal and external operational, financial, compliance and other risks facing Tameside Metropolitan Borough Council which may affect the audit, including the likelihood of those risks materialising and how they are monitored and managed.

With that in mind, we see this document, which has been prepared following our initial planning discussions with management, as being the basis for a discussion around our audit approach, any questions, concerns or input you may have on our approach or role as auditor. This document also contains an appendix that outlines our key communications with you during the course of the audit, and explains the implications of the introduction of the new auditing standard for Identifying and assessing the risks of material misstatement: ISA (UK) 315 (Revised 2019).

Client service is extremely important to us and we strive to provide technical excellence with the highest level of service quality, together with continuous improvement to exceed your expectations so, if you have any concerns or comments about this document or audit approach, please contact me on +44 (0)161 238 9349.

Yours faithfully



Daniel Watson

Mazars LLP

Mazars LLP – One St Peter's Square, Manchester, M2 3DE

Tel: +44 (0)161 238 9200 – www.mazars.co.uk

Mazars LLP is the UK firm of Mazars, an integrated international advisory and accountancy organisation. Mazars LLP is a limited liability partnership registered in England and Wales with registered number OC308299 and with its registered office at 30 Old Bailey, London EC4M 7AU.

We are registered to carry on audit work in the UK by the Institute of Chartered Accountants in England and Wales. Details about our audit registration can be viewed at www.auditregister.org.uk under reference number C001139861. VAT number: 839 8356 73

01

Section 01:

Engagement and responsibilities summary

Page 14

1. Engagement and responsibilities summary

Overview of engagement

We are appointed to perform the external audit of Tameside Metropolitan Borough Council ('the Council') for the year to 31 March 2023. The scope of our engagement is set out in the Statement of Responsibilities of Auditors and Audited Bodies, issued by Public Sector Audit Appointments Ltd ('PSAA') available from the PSAA website: <https://www.psa.co.uk/managing-audit-quality/statement-of-responsibilities-of-auditors-and-audited-bodies/>. Our responsibilities are principally derived from the Local Audit and Accountability Act 2014 (the 2014 Act) and the Code of Audit Practice issued by the National Audit Office ('NAO'), as outlined below.

Audit opinion

We are responsible for forming and expressing an opinion on whether the financial statements are prepared, in all material respects, in accordance with the Code of Practice on Local Authority Accounting. Our audit does not relieve management or the Audit Panel, as those charged with governance, of their responsibilities.

The Director of Resources is responsible for the assessment of whether it is appropriate for the Council to prepare its accounts on a going concern basis. As auditors, we are required to obtain sufficient appropriate audit evidence regarding, and conclude on: a) whether a material uncertainty related to going concern exists; and b) consider the appropriateness of the Director of Resources' use of the going concern basis of accounting in the preparation of the financial statements.

Value for money

We are also responsible for forming a commentary on the arrangements that the Council has in place to secure economy, efficiency and effectiveness in its use of resources. We discuss our approach to Value for Money work further in section 5 of this report.



Fraud

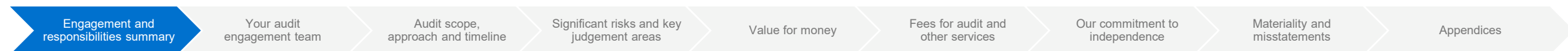
The responsibility for safeguarding assets and for the prevention and detection of fraud, error and non-compliance with law or regulations rests with both those charged with governance and management. This includes establishing and maintaining internal controls over reliability of financial reporting.

As part of our audit procedures in relation to fraud we are required to enquire of those charged with governance, including key management, as to their knowledge of instances of fraud, the risk of fraud and their views on internal controls that mitigate the fraud risks. In accordance with International Standards on Auditing (UK), we plan and perform our audit so as to obtain reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error. However our audit should not be relied upon to identify all such misstatements.

Wider reporting and electors' rights

We report to the NAO on the consistency of the Council's financial statements with its Whole of Government Accounts ('WGA') submission.

The 2014 Act requires us to give an elector, or any representative of the elector, the opportunity to question us about the accounting records of the Council and consider any objection made to the accounts. We also have a broad range of reporting responsibilities and powers that are unique to the audit of local authorities in the United Kingdom.



02

Section 02:

Your audit engagement team

2. Your audit engagement team

Below is your audit engagement team and their contact details.



Daniel Watson
Director

Email: daniel.watson@mazars.co.uk
Telephone: +44 (0)161 238 9349



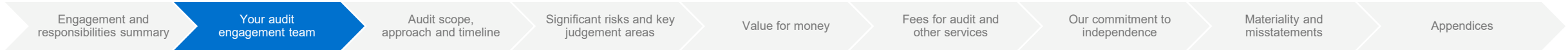
Ian Gilroy
Manager

Email: ian.gilroy@mazars.co.uk
Telephone: +44 (0)161 238 9347



Gareth Maher
Senior

Email: gareth.maher@mazars.co.uk
Telephone: +44 (0)161 238 9223



03

Section 03:

Audit scope, approach and timeline

Page 18

3. Audit scope, approach and timeline

Audit scope

Our audit approach is designed to provide an audit that complies with all professional requirements.

Our audit of the financial statements will be conducted in accordance with International Standards on Auditing (UK), relevant ethical and professional standards, our own audit approach and in accordance with the terms of our engagement. Our work is focused on those aspects of your activities which we consider to have a higher risk of material misstatement, such as those impacted by management judgement and estimation, application of new accounting standards, changes of accounting policy, changes to operations or areas which have been found to contain material errors in the past.

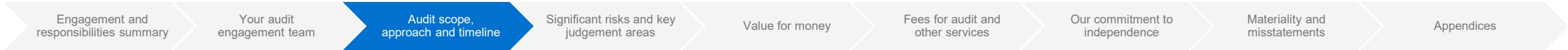
Audit approach

Our audit approach is risk-based and primarily driven by the issues that we consider lead to a higher risk of material misstatement of the accounts. Once we have completed our risk assessment, we develop our audit strategy and design audit procedures in response to the risks identified.

If we conclude that appropriately-designed controls are in place then we may plan to test and rely upon these controls. If we decide controls are not appropriately designed, or we decide it would be more efficient to do so, we may take a wholly substantive approach to our audit testing. Substantive procedures are audit procedures designed to detect material misstatements at the assertion level and comprise: tests of details (of classes of transactions, account balances, and disclosures); and substantive analytical procedures. Irrespective of the assessed risks of material misstatement, which take into account our evaluation of the operating effectiveness of controls, we are required to design and perform substantive procedures for each material class of transactions, account balance, and disclosure.

Our audit will be planned and performed so as to provide reasonable assurance that the financial statements are free from material misstatement and give a true and fair view. The concept of materiality and how we define a misstatement is explained in more detail in section 8.

The diagram on the next page outlines the procedures we perform at the different stages of the audit.



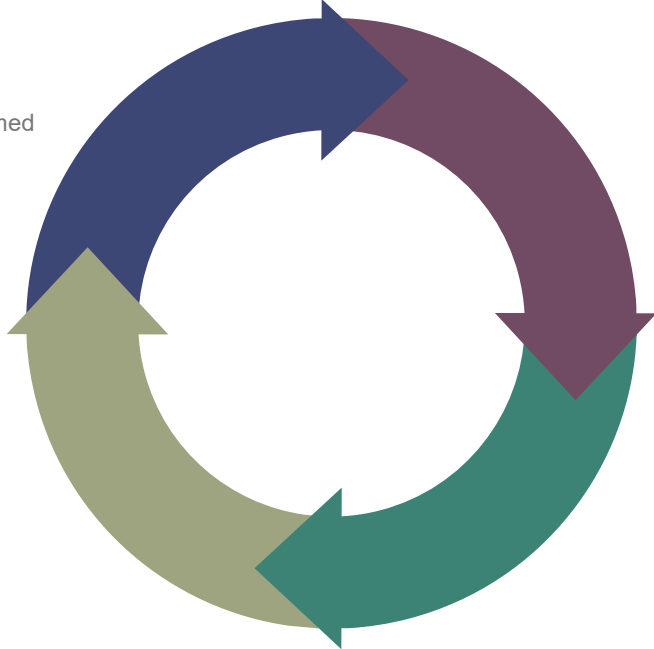
3. Audit scope, approach and timeline

Please note: this timeline is indicative of our approach to deliver the 2022/23 audit. This is dependent on the outcome on the backlog consultation and the finalisation of the 2021/22 audit.

Page 20

Planning and Risk Assessment - February 2024

- Planning visit and developing our understanding of the Council
- Initial opinion and value for money risk assessments
- Considering proposed accounting treatments and accounting policies
- Developing the audit strategy and planning the audit work to be performed
- Agreeing timetable and deadlines
- Risk assessment analytical procedures
- Determination of materiality



Interim - April 2024

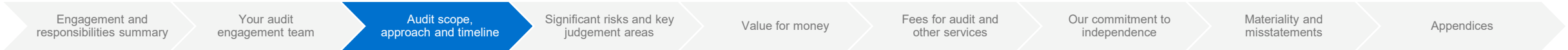
- Documenting systems and controls
- Performing walkthroughs
- Interim controls testing including tests of IT general controls
- Early substantive testing of transactions
- Reviewing draft financial statements
- Technical review of the draft financial statements
- Reassessment of audit plan and revision if necessary

Completion - September 2024

- Final review and disclosure checklist of financial statements
- Final director review
- Agreeing content of letter of representation
- Reporting to the Audit Panel
- Reviewing subsequent events
- Signing the independent auditor's report

Fieldwork – July to September 2024

- Delivering our audit strategy starting with significant risks and high risk areas including detailed testing of transactions, account balances and disclosures
- Communicating progress and issues
- Clearance meeting



3. Audit scope, approach and timeline

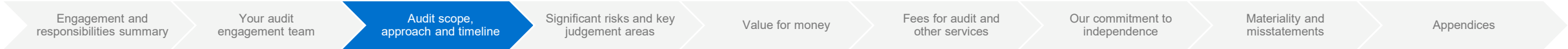
Reliance on internal audit

We do not intend to rely on the work of your internal audit team, but will review the work performed by the team to advise our audit strategy, and where appropriate modify the nature, extent and timing of our audit procedures. In addition, we will meet with internal audit to discuss and significant findings from their work.

Management’s and our experts

Management makes use of experts in specific areas when preparing the Council’s financial statements. We also use experts to assist us to obtain sufficient appropriate audit evidence on specific items of account.

Item of account	Management’s expert	Our expert
Property, plant and equipment and Investment properties – Valuations	Align Property Partners	We will engage our Mazars Property Valuations team to provide expertise on the complex valuations made by management’s expert.
Investment properties - Valuation of Manchester Airport Land	Colliers International Property Consultants Limited	We have appointed an external valuation expert to review the work of Colliers.
Long-term investments - Valuation of shareholdings in Manchester Airport Holdings Ltd	BDO LLP	Mazars Valuations Team
Defined benefit liability	Hymans Robertson – Actuary for the Greater Manchester Pension Fund	PwC, Consulting Actuary, on behalf of the NAO
Financial instrument disclosures	Arlingclose	We will review the methodology applied by Arlingclose to gain assurance that the fair value disclosures of the Council’s financial assets and liabilities are materially correct.



04

Section 04:

Significant risks and other key judgement areas

Page 22

4. Significant risks and other key judgement areas

Following the risk assessment approach discussed in section 3 of this document, we have identified risks relevant to the audit of financial statements. The risks that we identify are categorised as significant, enhanced or standard. The definitions of the level of risk rating are given below:

Significant risk

Significant risks are those risks assessed as being close to the upper end of the spectrum of inherent risk, based on the combination of the likelihood of a misstatement occurring and the magnitude of any potential misstatement. Fraud risks are always assessed as significant risks as required by auditing standards, including management override of controls and revenue recognition.

Enhanced risk

An enhanced risk is an area of higher assessed risk of material misstatement at audit assertion level other than a significant risk. Enhanced risks require additional consideration but does not rise to the level of a significant risk, these include but may not be limited to:

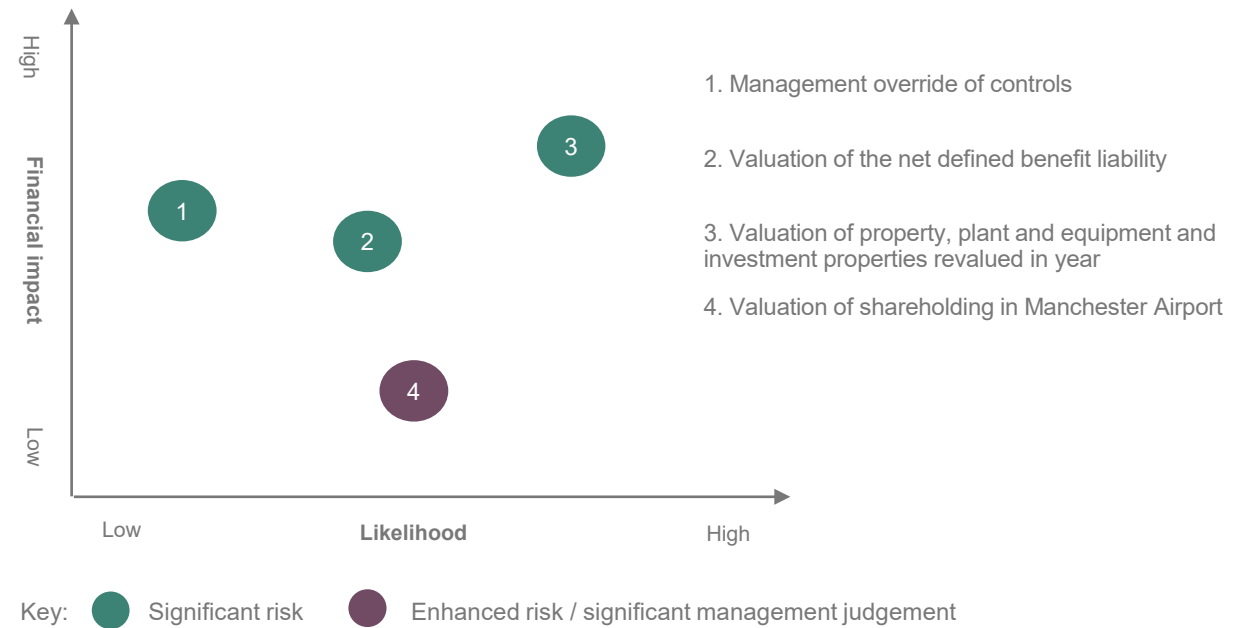
- Key areas of management judgement, including accounting estimates which are material but are not considered to give rise to a significant risk of material misstatement; and
- Other audit assertion risks arising from significant events or transactions that occurred during the period.

Standard risk

This is related to relatively routine, non-complex transactions that tend to be subject to systematic processing and require little management judgement. Although it is considered that there is a risk of material misstatement (RMM), there are no elevated or special factors related to the nature, the likely magnitude of the potential misstatements or the likelihood of the risk occurring.

Summary risk assessment

The summary risk assessment, illustrated in the table below, highlights those risks which we deem to be significant and other enhanced risks in respect of the Council. We have summarised our audit response to these risks on the next page.



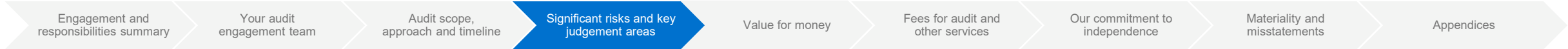
4. Significant risks and other key judgement areas

Specific identified audit risks and planned testing strategy

We have presented below in more detail the reasons for the risk assessment highlighted above, and also our testing approach with respect to significant risks. An audit is a dynamic process, should we change our view of risk or approach to address the identified risks during the course of our audit, we will report this to the Audit Panel.

Significant risks

	Description	Fraud	Error	Judgement	Planned response
1 Page 24	<p>Management override of controls This is a mandatory significant risk on all audits due to the unpredictable way in which such override could occur.</p> <p>Management at various levels within an organisation are in a unique position to perpetrate fraud because of their ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Due to the unpredictable way in which such override could occur there is a risk of material misstatement due to fraud on all audits.</p>	●	○	○	<p>We plan to address the management override of controls risk through performing audit work over:</p> <ul style="list-style-type: none"> • accounting estimates; • journal entries; and • significant transactions outside the normal course of business or otherwise unusual.

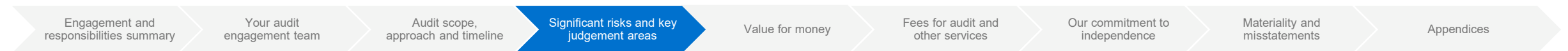


4. Significant risks and other key judgement areas

Significant risks

	Description	Fraud	Error	Judgement	Planned response
2	<p>Valuation of the net defined benefit liability £0.0m (2021/22: £252.8m)</p> <p>Previously the Council's accounts contained material liabilities relating to the local government pension scheme administered by the Greater Manchester Pension Fund (GMPF). In the 2022/23 year, the gross assets and liabilities remain material, however the net position is reported as a nil balance following the amendment for the asset ceiling.</p> <p>The Council and its subsidiaries rely upon an Actuary, Hymans Robertson, to provide an annual valuation of these liabilities in line with the requirements of IAS 19 Employee Benefits. Due to the high degree of estimation uncertainty associated with this valuation, we have determined there is a significant risk in this area.</p>	○	●	●	<p>We will evaluate the design and implementation of any controls which mitigate the risk. In addition our procedures will include:</p> <ul style="list-style-type: none"> • corresponding with the GMPF auditor to gain assurance on their audit of the Fund; • assessing the skill, competence and experience of the Fund's Actuary, including a review of the Actuary by our auditor external expert; • challenging the reasonableness of the assumptions used by the Actuary as part of the annual IAS 19 valuation; • reviewing the appropriateness of the pension asset and liability valuation methodologies applied by the Actuary, and the key assumptions included within the valuation. This will include comparing them to expected ranges, utilising information provided by our auditor external expert; • reviewing the appropriateness of the calculation of the asset ceiling under the relevant financial reporting standards, including a review of the key assumptions used in the calculation; and • carrying out a range of substantive procedures on relevant information and cash flows used by the Actuary as part of the annual IAS 19 valuation.

Page 25



4. Significant risks and other key judgement areas

Significant risks

	Description	Fraud	Error	Judgement	Planned response
3	<p>Valuation of property, plant and equipment and investment properties revalued in year £379.4m (2021/22: £83.6m)</p> <p>The Council's accounts contain material balances and disclosures relating to its holding of surplus assets and investment properties, which are required to be carried at fair value. Due to the high degree of estimation uncertainty associated with these valuations, we have determined there is a significant risk in the valuations of these property assets.</p>	○	●	●	<p>We will evaluate the design and implementation of any controls which mitigate the risk. In addition our procedures will include:</p> <ul style="list-style-type: none"> • assessing the skill, competence and experience of the Council's external valuer; • reviewing the instructions issued to the external valuer by management to ensure they comply with the Code requirements; • consider whether the overall revaluation methodology used by the Council's valuer is in line with industry practice, the CIPFA Code of Practice and the Council's accounting policies; • testing the valuations of a sample of properties; and • testing a sample of items of capital expenditure to confirm that the additions are appropriately valued in the financial statements.

Page 26

Other key areas of management judgement and enhanced risks

	Description	Fraud	Error	Judgement	Planned response
4	<p>Valuation of shareholding in Manchester Airport £24.4m (2021/22: £23.4m)</p> <p>The Council uses an external valuation expert to determine the value of its investment in Manchester Airport Holdings Limited as at 31 March 2023.</p> <p>The valuation is determined according to a methodology and applying assumptions. Council officers challenge the valuation assumptions and reach judgements on the valuation to include in the financial statements.</p>	○	●	●	<p>We plan to address this risk by:</p> <ul style="list-style-type: none"> • Assessing the scope of work / terms of engagement, qualifications, objectivity and independence of the expert engagement to carry out the valuation assessment of the airport shares. • Utilising the services of our internal valuation expert to review the work completed by management's expert and evaluate the appropriateness of the assumptions applied to arrive at the figure in the financial statements.

Engagement and responsibilities summary

Your audit engagement team

Audit scope, approach and timeline

Significant risks and key judgement areas

Value for money

Fees for audit and other services

Our commitment to independence

Materiality and misstatements

Appendices

05

Section 05: **Value for money**

5. Value for money

The framework for Value for Money work

We are required to form a view as to whether the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources. The NAO issues guidance to auditors that underpins the work we are required to carry out in order to form our view, and sets out the overall criterion and sub-criteria that we are required to consider.

2022/23 will be the third audit year where we are undertaking our value for money (VFM) work under the 2020 Code of Audit Practice (the Code). Our responsibility remains to be satisfied that the Council has proper arrangements in place and to report in the audit report and/or the audit completion certificate where we identify significant weaknesses in arrangements. Separately we provide a commentary on the Council's arrangements in the Auditor's Annual Report.

Specified reporting criteria

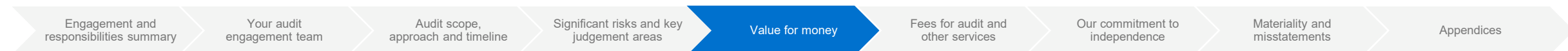
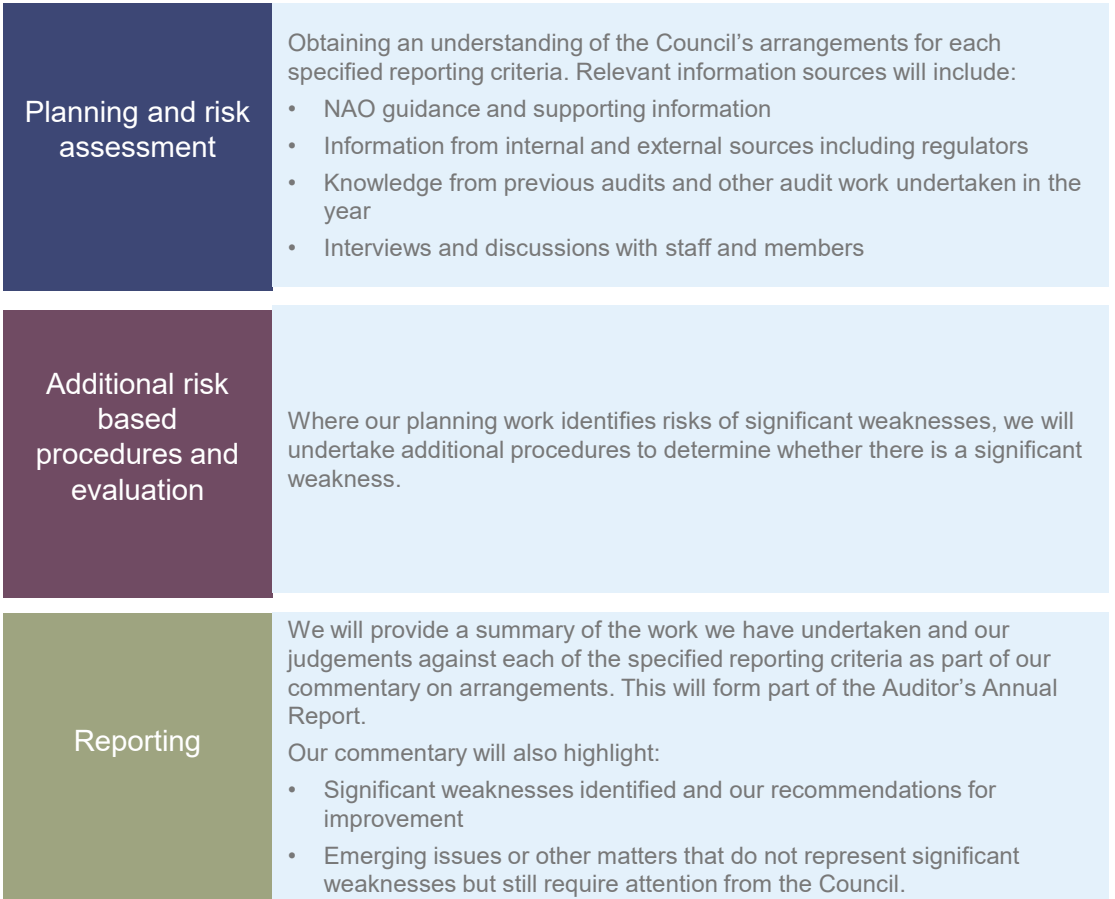
The Code requires us to structure our commentary to report under three specified criteria:

1. **Financial sustainability** – how the Council plans and manages its resources to ensure it can continue deliver its services
2. **Governance** – how the Council ensures that it makes informed decisions and properly manages its risks
3. **Improving economy, efficiency and effectiveness** – how the Council uses information about its costs and performance to improve the way it manages and delivers its services

Our approach

Our work falls into three primary phases as outlined opposite. We need to gather sufficient evidence to support our commentary on the Council's arrangements and to identify and report on any significant weaknesses in arrangements. Where significant weaknesses are identified we are required to report these to the Council and make recommendations for improvement. Such recommendations can be made at any point during the audit cycle and we are not expected to wait until issuing our overall commentary to do so.

In 2020/21 and 2021/22 we identified significant weaknesses arising from our audit process in relation to the preparation of the Council's financial statements. We will follow up on this weakness in 2022/23. We are also finalising our 21/22 value for money work which could give rise to additional issues. Should we identify any further risks during the course of the audit, we will report these to Audit Panel through our update reports.



06

Section 06:

Fees for audit and other services

Page 29

6. Fees for audit and other services

Fees for work as the Council's appointed auditor

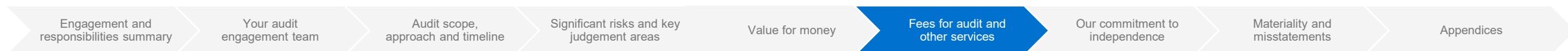
At this stage of the audit we are not planning any divergence from the scale fees set by PSAA as communicated in our fee letter.

Area of work	2022/23 Proposed Fee	2021/22 Estimated Fee
Scale fee – code audit work	£101,422*	£80,863
Additional fees in respect of:		
- Testing on Property, plant and equipment as a result of changes in regulatory expectations	-	£18,750
- Testing on Property, plant and equipment due to the Council applying the statutory override	-	£10,000
- Testing on Defined Benefit Pensions Schemes as a result of changes in regulatory expectations	-	£6,250
- Testing as a result of the implementation of new auditing standards: ISA 220 (Revised): Quality control of an audit of financial statements; ISA 540 (Revised): Auditing accounting estimates and related disclosures; ISA570 (Revised) Going Concern; and ISA 600 (Revised): Specific considerations – audit of group financial statements	£2,500	£2,500
- Additional Value for Money work arising from the change in the Code of Audit Practice	£12,500	£12,500
- Additional Value for Money work arising from risks of significant weaknesses in the Council's arrangements	TBC	£8,000
- Quality issues with the draft financial statements and errors identified during audit testing	TBC	TBC
Total fees	TBC	TBC

*There is an uplift from the 2021/22 scale fee by £20,559; of which £5,013 relates to the inflationary increase funded by PSAA, and £15,546 relates to adjustments for recurrent fee variations.

Fees for non-PSAA work

We have not been engaged by the Council to carry out additional work separate from our delivery of the NAO Code of Practice audit work. Before agreeing to undertake any additional work, we will consider whether there are any actual, potential or perceived threats to our independence. Further information about our responsibilities in relation to independence is provided in section 7.



07

Section 07:

Our commitment to independence

Page 31

7. Our commitment to independence

We are committed to independence and are required by the Financial Reporting Council to confirm to you at least annually in writing that we comply with the FRC's Ethical Standard. In addition, we communicate any matters or relationship which we believe may have a bearing on our independence or the objectivity of the audit team.

Based on the information provided by you and our own internal procedures to safeguard our independence as auditors, we confirm that in our professional judgement there are no relationships between us and any of our related or subsidiary entities, and you and your related entities creating any unacceptable threats to our independence within the regulatory or professional requirements governing us as your auditors.

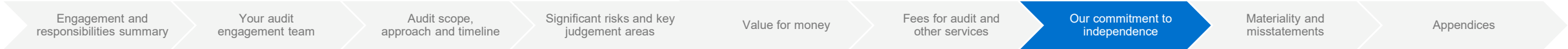
We have policies and procedures in place which are designed to ensure that we carry out our work with integrity, objectivity and independence. These policies include:

- all partners and staff are required to complete an annual independence declaration;
- all new partners and staff are required to complete an independence confirmation and also complete computer based ethical training;
- rotation policies covering audit engagement partners and other key members of the audit team; and
- approval by managers and partners of our client and engagement acceptance system which requires all non-audit services to be approved in advance by the audit engagement partner.

We confirm, as at the date of this document, that the engagement team and others in the firm as appropriate, Mazars LLP are independent and comply with relevant ethical requirements. However, if at any time you have concerns or questions about our integrity, objectivity or independence please discuss these with Daniel Watson in the first instance.

Prior to the provision of any non-audit services Daniel Watson will undertake appropriate procedures to consider and fully assess the impact that providing the service may have on our auditor independence.

Any emerging independence threats and associated identified safeguards will be communicated in our Audit Completion Report.



08

Section 08:

Materiality and misstatements

Page 33

8. Materiality and misstatements

Summary of initial materiality thresholds

Threshold	Initial threshold £'000s
Overall materiality	12,700
Performance materiality	8,200
Trivial threshold for errors to be reported to the Audit Panel	380
Specific materiality in relation to Senior Officer Remuneration	5

Materiality

Materiality is an expression of the relative significance or importance of a particular matter in the context of financial statements as a whole.

Information is considered to be material if omitting, misstating or obscuring it could reasonably be expected to influence the decisions that the primary users of general purpose financial statements make on the basis of those financial statements, which provide financial information about a specific reporting entity.

Judgements on materiality are made in light of surrounding circumstances and are affected by the size and nature of a misstatement, or a combination of both. Judgements about materiality are based on consideration of the common financial information needs of users as a group and not on specific individual users.

the financial information needs of the users of the financial statements. In making our assessment we assume that users:

- have a reasonable knowledge of business, economic activities and accounts;
- have a willingness to study the information in the financial statements with reasonable diligence;
- understand that financial statements are prepared, presented and audited to levels of materiality;
- recognise the uncertainties inherent in the measurement of amounts based on the use of estimates, judgement and the consideration of future events; and
- will make reasonable economic decisions on the basis of the information in the financial statements.

We consider materiality whilst planning and performing our audit based on quantitative and qualitative factors.

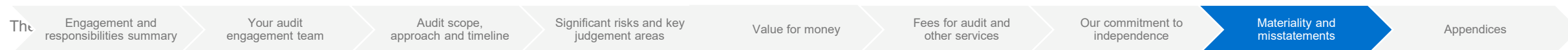
Whilst planning, we make judgements about the size of misstatements which we consider to be material and which provides a basis for determining the nature, timing and extent of risk assessment procedures, identifying and assessing the risk of material misstatement and determining the nature, timing and extent of further audit procedures.

The materiality determined at the planning stage does not necessarily establish an amount below which uncorrected misstatements, either individually or in aggregate, will be considered as immaterial.

We revise materiality for the financial statements as our audit progresses should we become aware of information that would have caused us to determine a different amount had we been aware of that information at the planning stage.

Our provisional materiality is set based on a benchmark of gross revenue expenditure at the surplus or deficit on provision of services level. We will identify a figure for materiality but identify separate levels for procedures designed to detect individual errors, and also a level above which all identified errors will be reported to the Audit Panel.

We consider that gross revenue expenditure at the surplus or deficit on provision of services remains the key focus of users of the financial statements and, as such, we base our materiality levels around this benchmark.



8. Materiality and misstatements

Materiality (continued)

We expect to set a materiality threshold at 2% of gross revenue expenditure at the surplus or deficit on the provision of services. Based on the draft financial statements of the Council, we anticipate the overall materiality for the year ending 31 March 2023 to be in the region of £12.7m (£11.9m in the prior year).

After setting initial materiality, we continue to monitor materiality throughout the audit to ensure that it is set at an appropriate level.

Performance Materiality

Performance materiality is the amount or amounts set by the auditor at less than materiality for the financial statements as a whole to reduce, to an appropriately low level, the probability that the aggregate of uncorrected and undetected misstatements exceeds materiality for the financial statements as a whole.

Our assessment of performance materiality is based on the findings of our planning and risk assessment procedures, including updating our understanding of the Council, the prior year audits and other factors. The outcome of these procedures has led to the audit team applying 65% of overall materiality as performance materiality.

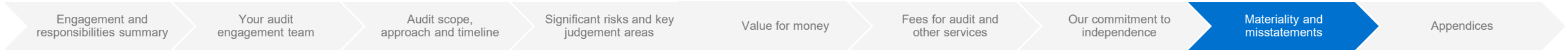
Misstatements

We accumulate misstatements identified during the audit that are other than clearly trivial. We set a level of triviality for individual errors identified (a reporting threshold) for reporting to the Audit Panel that is consistent with the level of triviality that we consider would not need to be accumulated because we expect that the accumulation of such amounts would not have a material effect on the financial statements. Based on our preliminary assessment of overall materiality, our proposed triviality threshold is £0.38m based on 3% of overall materiality. If you have any queries about this please do not hesitate to raise these with Daniel Watson.

Reporting to the Audit Panel

The following three types of audit differences above the trivial threshold will be presented to the Audit Panel:

- summary of adjusted audit differences;
- summary of unadjusted audit differences; and
- summary of disclosure differences (adjusted and unadjusted).





Appendices

A: Key communication points

B: Revised auditing standard on Identifying and assessing the risks of material misstatement: ISA (UK) 315 (Revised 2019)

Page 36

Appendix A: Key communication points

We value communication with Those Charged With Governance as a two way feedback process at the heart of our client service commitment. ISA 260 (UK) 'Communication with Those Charged with Governance' and ISA 265 (UK) 'Communicating Deficiencies In Internal Control To Those Charged With Governance And Management' specifically require us to communicate a number of points with you.

Relevant points that need to be communicated with you at each stage of the audit are outlined below.

Form, timing and content of our communications

We will present the following reports:

- Audit Strategy Memorandum;
- Audit Completion Report; and
- Auditor's Annual Report.

These documents will be discussed with management prior to being presented to yourselves and their comments will be incorporated as appropriate.

Key communication points at the planning stage as included in this Audit Strategy Memorandum

- Our responsibilities in relation to the audit of the financial statements;
- The planned scope and timing of the audit;
- Significant audit risks and areas of management judgement;
- Our commitment to independence;

- Responsibilities for preventing and detecting errors;
- Materiality and misstatements; and
- Fees for audit and other services.

Key communication points at the completion stage to be included in our Audit Completion Report

- Significant deficiencies in internal control;
- Significant findings from the audit;
- Significant matters discussed with management;
- Significant difficulties, if any, encountered during the audit;
- Qualitative aspects of the entity's accounting practices, including accounting policies, accounting estimates and financial statement disclosures;
- Our conclusions on the significant audit risks and areas of management judgement;
- Summary of misstatements;
- Management representation letter;
- Our proposed draft audit report; and
- Independence.

Engagement and responsibilities summary

Your audit engagement team

Audit scope, approach and timeline

Significant risks and key judgement areas

Value for money

Fees for audit and other services

Our commitment to independence

Materiality and misstatements

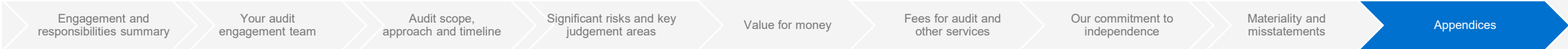
Appendices

Appendix A: Key communication points

ISA (UK) 260 'Communication with Those Charged with Governance', ISA (UK) 265 'Communicating Deficiencies In Internal Control To Those Charged With Governance And Management' and other ISAs (UK) specifically require us to communicate the following:

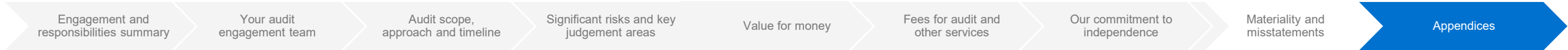
Required communication	Where addressed
Our responsibilities in relation to the financial statement audit and those of management and those charged with governance.	Audit Strategy Memorandum
The planned scope and timing of the audit including any limitations, specifically including with respect to significant risks.	Audit Strategy Memorandum
With respect to misstatements: <ul style="list-style-type: none"> • uncorrected misstatements and their effect on our audit opinion; • the effect of uncorrected misstatements related to prior periods; • a request that any uncorrected misstatement is corrected; and • in writing, corrected misstatements that are significant. 	Audit Completion Report
With respect to fraud communications: <ul style="list-style-type: none"> • enquiries of the Audit Panel to determine whether they have a knowledge of any actual, suspected or alleged fraud affecting the entity; • any fraud that we have identified or information we have obtained that indicates that fraud may exist; and • a discussion of any other matters related to fraud. 	Audit Completion Report and discussion at Audit Panel, Audit planning and clearance meetings

Page 38



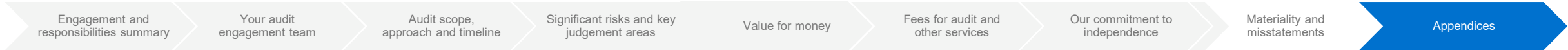
Appendix A: Key communication points

Required communication	Where addressed
Significant matters arising during the audit in connection with the entity's related parties including, when applicable: <ul style="list-style-type: none"> • non-disclosure by management; • inappropriate authorisation and approval of transactions; • disagreement over disclosures; • non-compliance with laws and regulations; and • difficulty in identifying the party that ultimately controls the entity. 	Audit Completion Report
Significant findings from the audit including: <ul style="list-style-type: none"> • Our view about the significant qualitative aspects of accounting practices including accounting policies, accounting estimates and financial statement disclosures; • significant difficulties, if any, encountered during the audit; • significant matters, if any, arising from the audit that were discussed with management or were the subject of correspondence with management; • written representations that we are seeking; • expected modifications to the audit report; and • other matters, if any, significant to the oversight of the financial reporting process or otherwise identified in the course of the audit that we believe will be relevant to the Audit Panel in the context of fulfilling their responsibilities. 	Audit Completion Report
Significant deficiencies in internal controls identified during the audit.	Audit Completion Report
Where relevant, any issues identified with respect to authority to obtain external confirmations or inability to obtain relevant and reliable audit evidence from other procedures.	Audit Completion Report



Appendix A: Key communication points

Required communication	Where addressed
Audit findings regarding non-compliance with laws and regulations where the non-compliance is material and believed to be intentional (subject to compliance with legislation on tipping off) and enquiry of the Audit Panel into possible instances of non-compliance with laws and regulations that may have a material effect on the financial statements and that the Audit Panel may be aware of.	Audit Completion Report and the Audit Panel meetings
With respect to going concern, events or conditions identified that may cast significant doubt on the entity's ability to continue as a going concern, including: <ul style="list-style-type: none"> • whether the events or conditions constitute a material uncertainty; • whether the use of the going concern assumption is appropriate in the preparation and presentation of the financial statements; and • the adequacy of related disclosures in the financial statements. 	Audit Completion Report
Reporting on the valuation methods applied to the various items in the annual financial statements including any impact of changes of such methods.	Audit Completion Report
Indication of whether all requested explanations and documents were provided by the Council.	Audit Completion Report



Appendix B: Revised auditing standard on Identifying and assessing the risks of material misstatement: ISA (UK) 315 (Revised 2019)

Background

ISA (UK) 315 (Revised 2019) introduces major changes to the auditor’s risk identification and assessment approach, which are intended to drive a more focused response from auditors undertaking work to obtain sufficient appropriate audit evidence to address the risks of material misstatement. The new standard is effective for periods commencing on or after 15 December 2021 and therefore applies in full for the Council’s 2022/23 audit.

The most significant changes relevant to the Council’s audit are outlined below.

Enhanced risk identification and assessment

The standard has enhanced the requirements for the auditor to understand the audited entity, its environment and the applicable financial reporting framework in order to identify and assess risk based on new inherent risk factors which include:

- Subjectivity
- Complexity
- Uncertainty and change
- Susceptibility to misstatement due to management bias or fraud.

Using these inherent risk factors, we assess inherent risk on a spectrum, at which the higher end of which lies significant risks, to drive an audit that is more focused on identified risks. Auditors are now also required to obtain sufficient, appropriate evidence from these risk identification and assessment procedures which means documentation and evidence requirements are also enhanced.

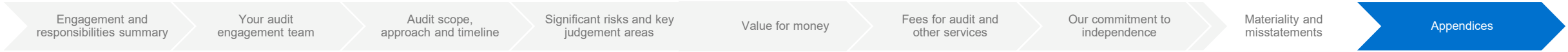
Greater emphasis on understanding IT

In response to constantly evolving business environments, the standard places an increased emphasis on the requirements for the auditor to gain an understanding of the entity’s IT environment to better understand the possible

risks within an entity’s information systems. As a result, we are required to gain a greater understanding of the IT environment, including IT general controls (ITGCs).

Increased focus on controls

Building on the need for auditors to gain a greater understanding of the IT environment, the standard also widens the scope of controls that are deemed relevant to the audit. We are now required to broaden our understanding of controls implemented by management, including ITGCs, as well as assess the design and implementation of those controls.



Contact

Mazars

One St Peters Square

M23DE

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.com

Follow us:

LinkedIn:

www.linkedin.com/company/Mazars

Twitter:

www.twitter.com/MazarsGroup

Facebook:

www.facebook.com/MazarsGroup

Instagram:


www.instagram.com/MazarsGroup

WeChat:

ID: Mazars

Agenda Item 5.

Report to:	AUDIT PANEL
Date:	12 March 2024
Executive Member/ Reporting Officer:	Cllr Jacqueline North – First Deputy (Finance, Resources & Transformation) Ashley Hughes – Director of Resources
Subject:	EXTERNAL AUDIT PROGRESS REPORT
Report Summary:	This report provides the Audit Panel with an update on the work undertaken by External Audit.
Recommendations:	Audit Panel are recommended to note the contents of the External Audit progress report.
Corporate Plan:	The report supports the Council's Corporate Plan objectives.
Policy Implications:	There are no direct policy implications flowing from the Statement of Accounts.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	An audited statement of accounts gives assurance on the Council's finances.
Legal Implications: (Authorised by the Borough Solicitor)	The requirement to externally audit the Council's statement of accounts is set out in the Accounts and Audit (England) Regulations 2015.
Risk Management:	The external audit provides verification of the financial statements.
Access to Information:	The report is to be considered in public.
Background Information:	The background papers relating to this report can be inspected by contacting Stuart Munro, Senior Finance Manager.

 Telephone: 0161 342 4257

 e-mail: stuart.munro@tameside.gov.uk

This page is intentionally left blank

Audit Progress Report

Tameside Metropolitan Borough Council

Page 45
Audit Panel
February 2024



1. Audit Progress
2. National publications

Page 46

01

Section 01: **Audit Progress**

Audit progress

Purpose of this report

This report provides the Audit, Governance and Standards Committee's with:

- a follow up on a question raised by members at the February 2024 Audit Panel meeting
- an update on the status of the financial statements audits for 2021/22
- an update on the status of the Value for Money work in respect of 2021/22;
- an update on the status of the Whole of Government Accounts work.

It also includes, at Section 2, a summary of recent national reports and publications for your information.

Follow up from the February Audit Panel

At the Audit Panel meeting in February we were asked to provide further information in respect of our internal control recommendation relating to leases.

We can confirm:

- our audit testing of leases covered a sample of 12.
- of those, two were found to be “holding over”
- these two leases are both with commercial tenants, and
- the leases expiries were May 2018 and March 2020 respectively.

We recommend the Council takes action to ensure lease agreements are reviewed and updated as they expire to ensure all properties leased out are subject to a contract. There is a risk the Council is not receiving the market rent for properties because rent reviews are not being undertaken. The Council is also open to other risks where the tenant does not have a current lease agreement in place.

Audit Progress

Status of the 2021/22 audit

As reported to members at the February Audit Panel, we have substantially completed our audit in respect of the financial statements for the year ended 31 March 2022. The table below sets out the progress on the audit areas which were reported as outstanding in our Audit Completion Report.

Audit area	Progress since February Audit Panel and outstanding matters
PPE – Impairments: Consideration of Reinforced Autoclaved Aerated Concrete (RAAC)	The Council provided evidence to show their consideration of the impact of RAAC on the asset portfolio and any potential impairments adjustments which may be required as a result of the presence of RAAC on Friday 12 January. Following our review of this consideration we requested further information from the Council on 19 January. A further response was provided on 23 February but at the time of issuing this report we have not received all of the required information. We will provide an update on the outcome of our review in our follow-up letter.
Financial statements, Annual Governance Statement and letter of representation	The Council will need to update the Annual Governance Statement for 2021/22 in light of the recent Ofsted report. At the time of issuing this report, we have not received an updated AGS to review. We will complete our final review of the financial statements upon receipt of the signed version of the accounts and letter of representation.

Page 49

Audit progress

Value for Money arrangements

We received the Council’s Value for Money self-assessment on 6 February 2024 with supporting evidence provided on 9 February. We are in the process of reviewing the evidence provided.

On 13 February Ofsted released a report following an inspection undertaken in December 2023. Following the inspection, Ofsted concluded that the overall effectiveness of the Council’s Children’s Services are Inadequate. Following the release of this report, we outline below the risk of significant weaknesses in arrangements that we have identified as part of our continuous planning procedures, and the work we intend to undertake in response:

Risk of significant weakness in arrangements	Planned response
<p data-bbox="78 619 137 772">Page 50</p> <p data-bbox="198 636 779 668">Ofsted Inspection: Children’s Services</p> <p data-bbox="198 715 1256 782">In February 2024 Ofsted issued a report following its inspection carried out between 4 and 15 December 2023 on the Council’s Services.</p> <p data-bbox="198 829 1289 896">The inspection report concluded that the overall effectiveness of the Council’s services is inadequate.</p> <p data-bbox="198 943 1200 1048">These matters indicate a risk of significant weaknesses in proper Arrangements in respect of governance and in respect of improving the economy, efficiency and effectiveness of services.</p>	<p data-bbox="1365 636 1811 668">To address this risk we plan to:</p> <ul data-bbox="1365 715 2435 858" style="list-style-type: none"><li data-bbox="1365 715 1918 746">• Review the Ofsted inspection report;<li data-bbox="1365 751 2435 818">• Hold discussions with management to understand the arrangements which were in place within the Children’s Services;<li data-bbox="1365 822 2359 858">• Review the Council’s response to the Ofsted report and action plan. <p data-bbox="1365 905 2168 936">We will report the findings of our work to the Audit Panel.</p>

Audit Progress

Whole of Government Accounts (WGA) work

We will submit the 2021/22 submission once we conclude the outstanding financial statements work.

Audit Progress 2022/23

Planning for the 2022/23 audit commenced on 12 February. Although our audit planning is being undertaken now, we are currently discussing with officers the impact of the Government's proposals for clearing the backlog on completion of the audit.

Further information on the 2022/23 audit progress will be provided in the 2022/23 Audit Strategy Memorandum.

02

Section 02:

National publications

National publications

This section highlights recent national publications that may be of interest to Members of the Panel. If you require any additional information, please contact any member of your engagement team.

We have, in the tables that follow, provided a brief insight into the purpose/key points of the publications with indicative relevance and/or suggested action using the following RAG ratings:

- Action required
- Action suggested
- For information only

	Publication/update	Key points	Link	Action
National Audit Office (NAO)				
Page 53 1 2 3 4	NAO insight – Financial Management in Government: Strategic Planning and Budgeting	The NAO has published a good practice guide in financial management aimed at senior finance leaders in government departments and other public bodies.	[here]	●
	Reforming Adult Social Care in England	This report looks at how DHSC is responding to the challenges facing adult social care in England, and its progress with delivering the reforms set out in the 2021 white paper.	[here]	●
	Approaches to Achieving Net Zero Across the UK	This report is a joint piece of work between the public audit offices of the four UK nations – Audit Scotland, Audit Wales, National Audit Office and Northern Ireland Audit Office – and has been produced with engagement from each respective government or administration. It sets out the UK and devolved governments’ legislation, policy, strategy, governance and monitoring arrangements, relevant to achieving net zero greenhouse gas emissions.	[here]	●
	Managing Risks in Government	By examining current practice in government and the private sector the NAO have developed six principles of risk management. By following these principles, organisations can move their risk management arrangements from a process-led approach to one which supports the efficient and effective delivery of services.	[here]	●

National publications (continued)

	Publication/update	Key points	Link	Action
Chartered Institute of Public Finance and Accountancy				
5	Section 114s: where are we headed next? 16 August 2023	Rob Whiteman, CIPFA CEO assesses the latest position on s114 notices (where formal action needs to be taken to balance a Council's finances), what has been done to prevent further s114 notices, whether more will occur and what the sector should do. This originally appeared as an article in the Municipal Journal on 31 July 2023.	[here]	●
Department for Levelling Up, Housing and Communities				
6	Municipal Journal Article by a Local Government Minister on Rebuilding Audit, 30 October 2023	An article by Lee Rowley MP in Municipal Journal and the most up-to-date statement at the current time of proposals to address the backlog of local government audits.	[here]	●
7	Addressing the local audit backlog in England: Consultation	This consultation seeks views on amending the Accounts and Audit Regulations 2015 as part of a package of cross-system measures to clear the backlog and put the system on a sustainable footing.	[here]	● Management should note the proposed arrangements
Mazars				
8	Mazars Transparency Report	We are pleased to present the 2022-2023 Transparency Report for Mazars in the UK. Our 2023 report provides an overview of how we are continuing to enhance audit quality within Mazars and contributing to safeguarding the public interest.	[here]	●

Contact

Mazars

Partner: Karen Murray

Email: karen.murray@mazars.co.uk

Senior Manager: Amelia Salford

Email: amelia.salford@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.com

Follow us:

LinkedIn:

www.linkedin.com/company/Mazars

Twitter:

www.twitter.com/MazarsGroup

Facebook:

www.facebook.com/MazarsGroup

Instagram:

www.instagram.com/MazarsGroup


WeChat:

ID: Mazars

This page is intentionally left blank

Agenda Item 6.

Report to:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Ashley Hughes – Director of Resources
Subject:	ANNUAL GOVERNANCE STATEMENT ACTIONS FOLLOW UP
Report Summary:	To present the Audit Panel with an update to the Annual Governance Statement Action Plan, and in accordance with best practice.
Recommendations:	That progress against the action plan at Appendix 1 is noted.
Corporate Plan:	Demonstrates Corporate Governance.
Policy Implications:	Demonstrates compliance with the Accounts and Audit Regulations 2015 (as amended).
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	Sound corporate governance and proper systems of internal control are essential for the long-term financial health and reputation of the Council.
Legal Implications: (Authorised by the Borough Solicitor)	Local authorities are required by the Accounts and Audit Regulations 2015 (as amended) to prepare a governance statement in order to report publicly on the extent to which the council is complying with its own code of governance on an annual basis, including the monitoring and evaluation of the effectiveness of the governance arrangements in the year. This report provides the half yearly report of progress against actions.
Risk Management:	The statement provides assurance that the Council has a sound system of corporate governance in place. It is considered to be an important public expression of how the Council directs and controls its functions and relates to its community.
Background Information:	The background papers relating to this report can be inspected by contacting Carol McDonnell, Head of Assurance

 0161 342 3231

 carol.mcdonnell@tameside.gov.uk

This page is intentionally left blank

APPENDIX 1

Annual Governance Statement 2022/2023 – Improvement Plan March 2024 UPDATE

Ref	Area of Review	Improvement Identified for Implementation in 2021/22 AGS	Progress Reported As At June 2023	Improvement Identified for Implementation in 2023/2024 Improvement Owner and Completion Date	UPDATE
1	Vision Tameside (Carry Forward)	To complete the Ashton Town Hall project along with the remaining elements of the Vision Tameside project. Director of Place March 2022 and ongoing	This project is part of Tameside's Levelling Up Funding proposals. Completion aim is March 2025.	Completion of project by March 2025. Director of Place March 2025	Still scheduled to be finished by March 2025.
2	Children's Services (Carry Forward)	To monitor the revised improvement plan with delivery action and risks being tracked monthly. Director of Children's Services March 2023	Complete and ongoing. Eight-month stock take of the improvement plan monthly actions RAG rated and approved and signed off May 23 by Children's Improvement Board Quarterly monitoring of Improvement Plan undertaken by Children's Scrutiny Panel.	Revised improvement plan coproduced with partners and signed off at Children's Improvement Board April 23 agreed with DFE. Monthly actions tracked into Improvement Board forward plan and agenda reports schedule. External DFE 6-month review of progress 20/06/23. Director Children's Services March 2024	Ofsted inspection completed in December 2023, with the report published in February 2024.

Ref	Area of Review	Improvement Identified for Implementation in 2021/22 AGS	Progress Reported As At June 2023	Improvement Identified for Implementation in 2023/2024 Improvement Owner and Completion Date	UPDATE
3	Management of CCTV (Carry Forward)	Capital investment to update the CCTV system as funding becomes available. Director of Place Autumn 2022	Action carried forward	Capital investment to update the CCTV system as funding becomes available. Assistant Director Place March 2025	Still on target to complete by March 2025.
4	ICT Disaster Recovery and Business Continuity Planning (Carry Forward)	Services to review and agree their system recovery priorities in conjunction with the IT Service. Once determined systems will need to be put in place to ensure Tier 1 systems have full recovery checks and tests undertaken annually and Tier 2 systems every other year. Director of Finance March 2023	Action carried forward	Services to review and agree their system recovery priorities in conjunction with the IT Service. Once determined systems will need to be put in place to ensure Tier 1 systems have full recovery checks and tests undertaken annually and Tier 2 systems every other year. Director of Resources March 2024	This work is programmed for Quarter 4 following the recruitment for the permanent Assistant Director – ICT & Digital in December 2023.
5	Information Governance (Carry Forward)	Delivery of the Information Governance Work Plan and review the Information Governance Service across the Council. Director of Governance and Pensions Director of Finance January 2023	Action carried forward	The Information Governance Work Plan has been regularly monitored in 2022/23 by the Information Governance Group. Capacity issues within the service has impacted upon progress. This will be addressed in 2023/24. Director of Resources Head of Assurance March 2024	The Information Governance Work Plan is monitored by the Information Governance Group. A few policies are due to be presented to Audit Panel in March 2024 as part of that work.

Ref	Area of Review	Improvement Identified for Implementation in 2021/22 AGS	Progress Reported As At June 2023	Improvement Identified for Implementation in 2023/2024 Improvement Owner and Completion Date	UPDATE
6	Implementation of a Strategic Commissioning Function (Carry Forward)	<p>Until the proposed legislation is passed through Parliament, it is difficult to evaluate the risks ahead.</p> <p>As further clarity is received on the GM Integrated Care System, risks will be identified, evaluated and reported in accordance with the joint principles agreed across the Place based leadership model.</p> <p>Director of Finance/Single Leadership Team September 2022</p>	Action no longer relevant due to changes in GM moving forward with locality-based leads.		
7	Debtors (Carry Forward)	<p>Improvements to the Debtors System need to be embedded across the Council and these will then be tested by Internal Audit in the latter half of 2022/23 to provide assurance that the overall system is working effectively and fit for purpose.</p> <p>Director of Governance and Pensions Director of Finance March 2023</p>	Action carried forward	<p>Debtors has been included on the refreshed audit plan for 2023/24 and will be completed by Quarter 2.</p> <p>Head of Assurance December 2023</p>	<p>Implemented. Debtors audit completed, report in draft.</p>

Ref	Area of Review	Improvement Identified for Implementation in 2021/22 AGS	Progress Reported As At June 2023	Improvement Identified for Implementation in 2023/2024 Improvement Owner and Completion Date	UPDATE
8	Compliance with the CIPFA Financial Management Code (Carry Forward)	To ensure that the nine improvements identified in the assessment conducted and reported to Executive Cabinet in April 2021 are implemented. Director of Finance March 2023	Action carried forward	A draft self-assessment was undertaken in June 2023 by Financial Management. This will be published in 2023/24 and reviewed by the Audit Panel as part of their 2023/24 work programme. Director of Resources September 2023	October 2023: The FM Code review is down on the audit plan for January 2024. It should be in the AGS going forward as part of the annual review. February 2024: FM Code presented to the Audit Panel.
9	Early Help Service (Carry Forward)	To review and implement the learning and improvements identified by the Peer Review conducted by Stockport Council in December 2020. Delivery of colocation of neighbourhood teams along with a newly identified Family Hubs work programme. Director of Children's Services December 2022	All learning and improvements implemented and responded to. Family Hubs launched and opened in January 23. New Early Help Strategy and delivery model agreed with Partners in May 23 due to be received at Cabinet June 23	As progress reported. Director of Children's Services June 2023	January 2024: The Family Hubs delivery plan has been approved by DFE and regular KIT meetings are held to ensure this is on track. Data returns are completed quarterly to DFE. The Early Help Strategy is in place and the delivery plan is currently being updated to share with the Early Help partnership, to utilise community services and create a whole system approach to Early Help.
10	Assurance (Risk & Audit)			Embed a model of assurance to the disciplines of risk and audit using the '3 lines approach'. Head of Assurance March 2024	Implemented Three lines introduced via new risk management process and integrated into audit planning approved by Audit Panel on 1 August 2023.

Ref	Area of Review	Improvement Identified for Implementation in 2021/22 AGS	Progress Reported As At June 2023	Improvement Identified for Implementation in 2023/2024 Improvement Owner and Completion Date	UPDATE
11	Statutory Accounts sign off			Liaison with External Audit to expedite sign off of outstanding statutory accounts. Director of Resources March 2024	2020/21 Accounts signed off. 2021/22 Accounts ACR presented to February 2024 Audit Panel. Statutory backstop consulted on for September 2024 for 2022/23 Accounts. Plan in place to deliver 2022/23 Accounts prior to backstop.
12	Medium Term Financial Strategy			Implementation of a robust medium term financial strategy. Director of Resources February 2024 (Budget Council)	MTFS reported to Cabinet in July, October and December 2023. 2024/25 budget balanced and out to consultation until 2 Feb 2024. MTFS underpinned by external support and commissioned transformation expertise.
13				Embed a refreshed strategic delivery and performance framework during 2023/24. Head of Policy, Performance & Intelligence March 2024	Implemented Framework outline agreed by Executive Cabinet in September 2023. See link below. Item 5 - agenda for Executive Cabinet on Wednesday, 27th September, 2023, 1.00 pm (modern.gov.co.uk) Subject to monitoring and considered embedded.

This page is intentionally left blank

Report To:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Carol McDonnell – Head of Assurance
Subject:	INFORMATION GOVERNANCE POLICIES
Report Summary:	This report presents the updated policies in respect of information governance.
Recommendations:	<ol style="list-style-type: none">1. Members approve the IT Security Policy shown at Appendix 1.2. Members approve the IT Acceptable Use Policy shown at Appendix 2.3. Members approve the Social Media Use: Responsible Conduct Policy shown at Appendix 3.
Corporate Plan:	Strong information governance supports the individual operations, which deliver the objectives of the Council.
Policy Implications:	The documents will add further guidance to the Data Protection / Information Governance Framework to enable staff to adhere to the requirements of the Data Protection Act 2018 and UK General Data Protection Regulations (GDPR).
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	<p>There is a significant financial risk to the Council for non-compliance with the Data Protection Act 2018 and UK GDPR as this can result in the Information Commissioner's Office (ICO) imposing financial penalties.</p> <p>For context, these can be up to a maximum of £17million or 4% of annual turnover (depending on which is larger) for the most serious breaches.</p> <p>In addition, data subjects impacted by data breaches can claim for damages, which can also result in a financial liability on the Council budget, the value of which will be dependent on the individual claim(s).</p>
Legal Implications: (Authorised by the Borough Solicitor)	Non-compliance with the Data Protection Act 2018 (as amended) and UK GDPR (General Data Protection Regulation) could expose the Council to enforcement action and/or financial penalties from the ICO, claims for damages from data subjects impacted by data breaches, as well as damage the Council reputationally.
Risk Management:	Information is a valuable asset to the Council and personal information needs to be protected as privacy failures could be very damaging to the Council in terms of reputational damage and significant financial implications. The necessity to update and refresh policies that are part of the Data Protection / Information Governance Framework is critical if we are to comply with the requirements of the Data Protection Act 2018 and UK GDPR.
Access to Information:	The background papers relating to this report can be obtained by contacting Carol McDonnell, Head of Assurance



0161 342 3231



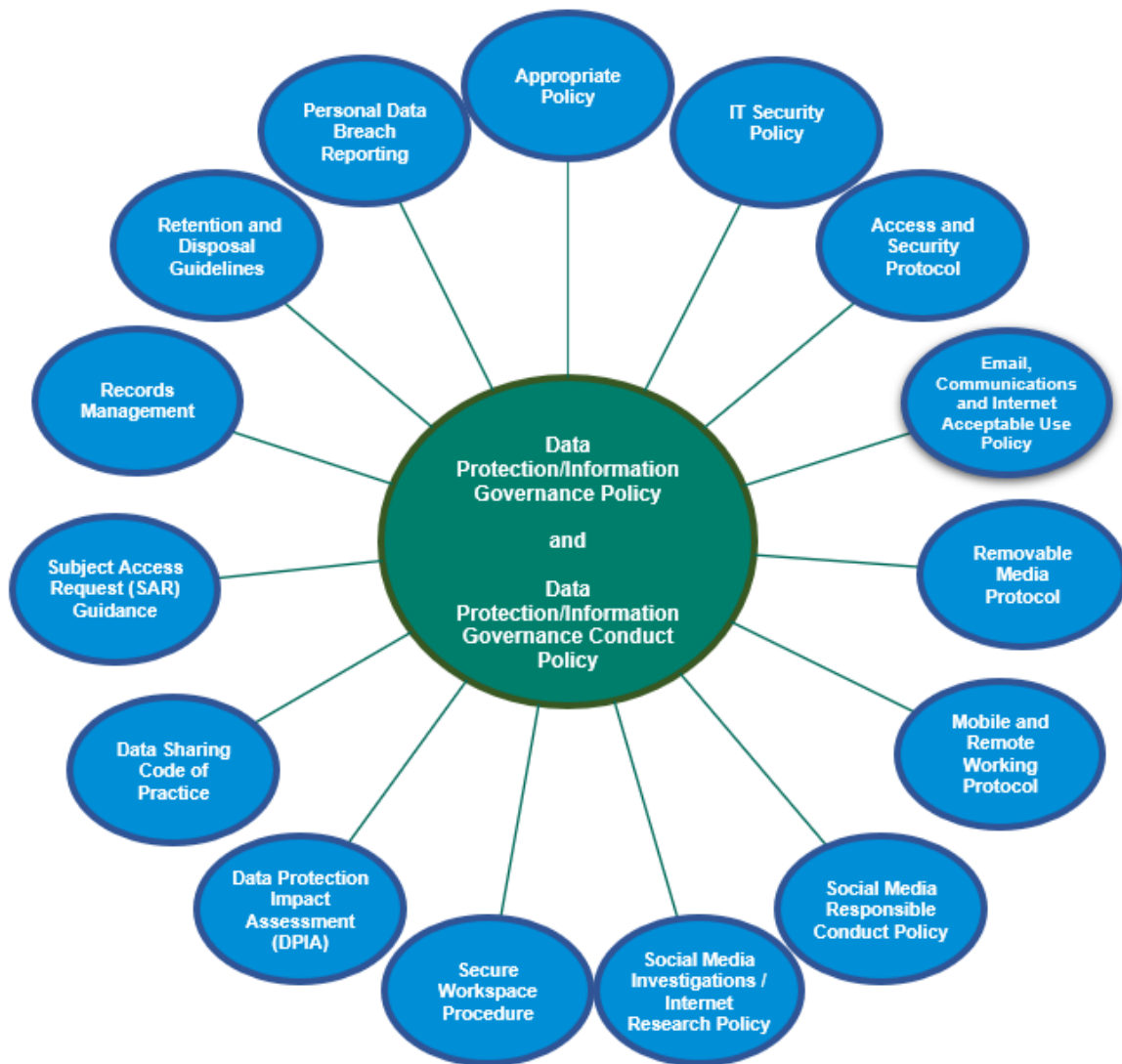
carol.mcdonnell@tameside.gov.uk

1. INTRODUCTION

- 1.1 Information Governance can mean different things to different people. It can be defined as the set of multi-disciplinary structures, policies, procedures, processes, and controls implemented to manage information, supporting the Council's immediate and future regulatory, legal, risk, environmental and operational requirements.
- 1.2 Information Governance can also describe the way we manage our obligations for: accessing information, reuse of information, records management, surveillance, data protection, information security, Information Technology (IT) security, etc.
- 1.3 The primary pieces of legislation relating to Information Governance and data protection are:
- Data Protection Act 2018 (DPA) – enables an applicant to access information of which they are the subject, e.g., someone's own education/social care records, employee files etc.
 - UK General Data Protection Regulations (UK GDPR) – like the EU GDPR, provides safeguards to individuals over the processing of their personal information and setting requirements for organisations to ensure appropriate technical and organisational measures are in place to comply with the principles of data protection.
- 1.4 The following lists some other legislation that impacts Information Governance:
- Freedom of Information Act 2000 (FOIA) – enables an applicant access to information which is held by/on behalf of public authorities and those bodies carrying out a public function, and which does not fall under either of the access regimes i.e., personal information or environmental information.
 - Environmental Information Regulations 2004 (EIR) – enables an applicant to access environmental information.
 - Privacy and Electronic Communications Regulations 2003 (PECR) – sets out privacy rights relating to electronic communications, and covers electronic marketing, the use of website cookies, the security of public electronic communications services and privacy of users of electronic communications services.
 - Re-use of Public Sector Information Regulations 2015 – establishes the UK framework for the re-use of public sector information. Accessible information which is produced, held, or disseminated by the public sector body must be made available for re-use (unless it is otherwise restricted or excluded).

2. DATA PROTECTION / INFORMATION GOVERNANCE FRAMEWORK

- 2.1 The Data Protection / Information Governance Framework comprises the policies and procedures of the Council, which relate to Information Governance, with the overarching document being the Data Protection / Information Governance Policy and the Data Protection / Information Governance Conduct Policy.
- 2.2 The following diagram details all the policies and procedures contained within the framework:



3. UPDATED FRAMEWORK DOCUMENTS

3.1 An Information Governance Workplan is in place, which is monitored by the Information Governance Group.

3.2 At the last meeting of the Information Governance Group, the following policies were reviewed:

- IT Security Policy – which sets out the Council’s policy on using its IT equipment and its internal and external infrastructure. The policy is located at **Appendix 1**.
- IT Acceptable Use Policy – which sets out what the various Council’s IT equipment can be used for, including permitted personal use, access controls, security, and compliance. The policy is located at **Appendix 2**.
- Social Media Policy – which sets out the expectations of officers and members in the use of social media as part of council duties as well as personal use. The policy is located at **Appendix 3**.

4. COMMUNICATIONS AND COMPLIANCE

- 4.1 Once the policies have been approved, steps will be taken to ensure that the new policies are effectively communicated to all staff, and to ensure compliance with policies is embedded.
- 4.2 It is proposed the Council takes the following steps:
- 4.3 Initial communications about the changes should be communicated through the Chief Executive's Weekly Briefing and posted on the Intranet outlining the key changes and what will happen as part of the user experience.
- 4.4 The log on screen 'Warning' message currently displayed at each log in will be updated to reflect the changes in this report. Users cannot log on without clicking OK to confirm their acceptance of the relevant policies.
- 4.5 A pop-up message will be displayed after signing in for the first time after the changes are implemented that will ask users to review the policies after providing a summary of the key changes. Users will be unable to progress further into the systems without indicating they have read and understood the policies and guidance.
- 4.6 Paper copies of the revised policies along with a paper briefing will be provided for all non-networked officers, e.g. officers based at the Depot at the same time as the system changes are made for IT users.
- 4.7 Lunch and learn sessions will be provided via Teams over a four-week period, allowing users multiple options to attend a live session. A similar session can be provided for non-networked officers if there is sufficient demand for one to be run.
- 4.8 One of the lunch and learn sessions will be recorded and uploaded to Me.Learning for any user that cannot attend the proposed sessions. It will also be available to new starters as part of the onboarding process during their probation periods.

5. RECOMMENDATIONS

- 5.1 As set out on the front of the report.



IT Security Policy

DRAFT

Date: December 2023

Version: V1.2

Document Version Control

Document Version Control		
Version Number	Date	Approved by
1.0	May 2018	Audit Panel
1.1	August 2021	N/a – consultation draft to HR/IG working group
1.2	December 2023	N/a – consultation draft to Information Governance Group

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

DRAFT

Contents

Document Version Control	2
1. INTRODUCTION.....	4
2. EQUIPMENT (EMPLOYEE RESPONSIBILITIES).....	4
3. EQUIPMENT (RETURN AND DISPOSAL).....	5
3.3. Staff Leavers	5
3.4. Internal movers.....	5
3.5. Moving equipment	6
4. TRAINING	6
5. MANAGEMENT OF DATA, INFORMATION AND SOFTWARE.....	6
6. AUTHORISED BUSINESS USE	6
7. UNAUTHORISED USE	7
8. SECURITY	7
8.1. Access to Council systems.....	7
8.2. Passwords	7
9. PERSONAL USE	8
10. THE COUNCIL'S RIGHTS AND OBLIGATIONS	8
11. CYBER SECURITY	9
11.3. Phishing	9
11.4. Malicious Software ('Malware')	9
12. USE OF IT AT HOME OR OUT OF THE OFFICE	10
13. BACK UPS	10
14. CONTRAVENTIONS OF THE POLICY.....	10
15. DISCIPLINARY IMPLICATIONS	10
16. PERSONAL DATA BREACH INCIDENTS	10
17. DEFINITIONS.....	11

1. INTRODUCTION

1.1. IT is an integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees use Council IT in the course of their duties. This policy is designed to enable the Council to:

- Preserve the confidentiality, integrity and availability of its data/information;
- Ensure an approach to security in which all employees fully understand their own responsibilities;
- Ensure that all employees are aware of and fully comply with the legislation as described in this and other policies;
- Minimise legal and other risks associated with the use of technology;
- Detail how to protect the data/information assets under the Council's control;
- Get the best return possible for the investment it has made in technology;
- Ensure effective running of the Council's business;
- Use technology to maximise flexibility around new working practices;
- Minimise the risk of disruption caused by malware and inappropriate use of IT; and
- Provide clear information to employees and increase the IT skills of our employees and residents.

1.2. This policy sets out the Council's policy on using its IT equipment and its internal and external infrastructure ('systems').

1.3. This policy applies to all Council employees who use the Council's equipment and systems.

2. EQUIPMENT (EMPLOYEE RESPONSIBILITIES)

2.1. All employees have responsibility for the equipment they use and the data/information accessed through and stored on that equipment. Everyone using Council equipment must adhere to the below points regarding Council Equipment and Data.

2.2. If equipment malfunctions you should contact the IT Service Desk for advice and assistance. Employees must not attempt to repair or maintain their IT equipment, except for day-to-day needs such as replacement ink cartridges in printers etc. All employees are expected to look after any Council equipment as if it was their own personal equipment, to ensure it is kept in good working order.

2.3. Employees are expected to make efforts to avoid circumstances that may result in accidental damage, such as spilt coffee or equipment being dislodged off desks. Smartphones will be provided with a protective case which must be used at all times. Any deliberate damage could result in the employee being personally liable for the cost of repair or replacement of the damaged equipment.

2.4. Damaged equipment must not be disposed of by individuals and should be returned promptly to IT Services. This is to ensure the safe removal of any licences or data from the device.

2.5. Employees are the last line of defence against cyber-attack. Every employee has a responsibility to use their equipment safely and responsibly to avoid exposing the Council's systems to cyber-attack.

2.6. Every employee has a duty to ensure that any and all equipment provided to them is kept secure from loss, theft or attack. This particularly applies to portable equipment such as laptop computers, tablets and mobile phones. The Council carries insurance for incidents

APPENDIX 1

beyond an employee's control within the UK, but if equipment is lost as a result of an employee's negligent or deliberate act then disciplinary action may be taken and the Council may take action to recover the cost from the employee concerned. Any queries about this should be referred to the Insurance Team (insurance@tameside.gov.uk).

- 2.7. Where the Council provides a laptop to an employee, it is the responsibility of the employee to ensure that the anti-virus updates and software updates that are automatically deployed to devices are promptly downloaded. This is achieved by regularly logging the device off (selecting "shut down" and waiting until the process is complete before closing the device).
- 2.8. All Council equipment must be purchased through IT Services using the Council's approved procurement facility. For the avoidance of doubt, it is not permitted for any manager or employee to purchase IT equipment themselves and reclaim the cost through the expense system. Any equipment not procured through IT Services poses a security risk to the integrity of the Council's systems and/or the data/information stored or processed on the unsanctioned piece of equipment.

3. EQUIPMENT (RETURN AND DISPOSAL)

- 3.1. All equipment must be disposed of through IT Services to ensure that legislation is complied with both in respect of the environment and security of information. Moving IT equipment or disposing of it without taking appropriate measures to keep information secure is likely to result in confidential information becoming available to persons not entitled to the data and consequentially breaches in legislation.
- 3.2. When IT Services receive equipment back, they will determine whether the equipment can be repurposed for further use within the Council, or is to be disposed of securely. Where equipment cannot be reused, it is disposed of via a third party contractor, who will comply with relevant industry standards to safely dispose of the equipment, meeting all regulatory and legislative requirements, including effective destruction of any data held on the equipment. Where the equipment can be repurposed, it will be securely wiped to ensure all data is removed before reallocation to another user.

3.3. Staff Leavers

- 3.3.1. Where an employee leaves the Council, the manager must follow the Leavers Checklist available via the intranet and must also log a "leaver request" through the IT Service Desk. This will ensure the correct system accesses are removed and the return of all equipment is arranged on the leaver's final working day or as soon after as is possible. Managers are accountable for making sure this is strictly complied with. Failure to return the equipment promptly to IT will result in a data breach being recorded against the manager and also could lead to the matter being reported to the police as stolen property. We reserve the right to seek recovery of replacement costs of equipment and associated costs from employee's. Please note that the service area is initially charged replacement cost for any non- returned equipment.

3.4. Internal movers

- 3.4.1. Where employees move internally between different service areas within the Council, the manager of the team being left has responsibility for notifying IT Services. The manager must follow the Movers Checklist available via the intranet and must also log a 'movers request' through the IT Service Desk.
- 3.4.2. The manager of the new team will log a "new starter" ticket on the IT Service Desk.
- 3.4.3. The full process for staff movers can be found in the [IT Acceptable Use Policy](#)

3.5. Moving equipment

- 3.5.1. Where equipment, such as desktop PCs, printers/scanners, servers etc. need to be relocated, IT Services must be contacted to carry this out. Equipment must only be moved by IT Services.

4. TRAINING

- 4.1. All employees are expected to undertake IT training, and mandatory Information Governance training as directed where they handle any data as part of their day to day role. The Information Governance training is required to be completed on an annual basis.
- 4.2. The IT Induction training is mandatory and will be provided to all new starters as they collect their IT equipment. IT equipment including passwords will not be issued until the induction has taken place. By exception (for example where a new starter does not live locally), equipment can be issued but passwords will be withheld until the induction has taken place either in person or remotely.

5. MANAGEMENT OF DATA, INFORMATION AND SOFTWARE

- 5.1. Employees are expected to manage data in compliance with the legislation relating to data protection and freedom of information. The Data Protection/Information Governance Framework and supporting policies, protocols, procedures and guidance documents <https://intranet2.tameside.gov.uk/infogov> provide additional support, but the main principles are that employees must:
 - Keep data accurate and up to date and retain for no longer than necessary, in line with the corporate [Retention and Disposal Guidance/Schedule](#)
 - Keep data secure
 - Keep data confidential.
- 5.2. The Council has legal duties under the Data Protection Act 2018 and Computer Misuse Act 1990 to protect the information that it holds. No personal information should be disclosed unless you are sure that you are permitted to do so and the appropriate data sharing or processing agreements are in place. If any employees have any further queries they should seek advice from the Information Governance Team (information.governance@tameside.gov.uk).

6. AUTHORISED BUSINESS USE

- 6.1. You may use the Council's systems where you have a legitimate business need to do so and the use is appropriate to your role or you are using the systems for appropriate personal use in accordance with section 10 of this policy.
- 6.2. Each day as you log onto your device you will be presented with a screen confirming you agree to comply with the Council's policies including but not limited to this Policy, the Acceptable Usage Policy and the Information Governance Policies.
- 6.3. In order to ensure accountability in the use of the Systems, you must only use the equipment you have been personally allocated by IT Services.

- 6.4. Employees may only use software officially purchased, issued and approved by IT Services as the Council is under an obligation to ensure that all software is properly licensed and approved and that the individual and business intellectual property rights in respect of that software are protected at all times. Users breaching this requirement may be subject to disciplinary action.

7. UNAUTHORISED USE

- 7.1. There are controls in place to ensure that employees cannot misuse the Council's systems or software. Employees must not use any software, including cloud service, which has not been officially purchased, issued or approved by IT Services and been through the DPIA process. Employees must not copy or attempt to copy any of the software on the Council's Systems. Software will be audited on a regular basis.
- 7.2. You must not connect any equipment to the Council's Systems unless it belongs to the Council and you have the express permission of IT Services.
- 7.3. You must not misuse the Council's Systems by accessing information which you are not authorised to view or use in performance of your duties. Access to any data for personal use is strictly prohibited and will result in disciplinary action. You must not attempt to break ('hack') into any computer system, for example by using someone else's password.

8. SECURITY

8.1. Access to Council systems

- 8.1.1. Maintaining the security of the Council's network and IT systems is vitally important. Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure only authorised user access and to prevent unauthorised access.
- 8.1.2. Each user must be allocated access rights and permissions to computer systems and data that:
- Are appropriate for the tasks they are expected to perform;
 - Have a unique login that is not shared with or disclosed to any other user;
 - Have an associated unique password that complies with the Council's password guidance (see section 9.2).
- 8.1.3. Where appropriate multi-factor authentication (MFA) will be added to Council systems as an additional layer of security.
- 8.1.4. User access rights must be reviewed at regular intervals to ensure that the privilege of least access is being implemented – that is that appropriate rights are only allocated to present employees of the service area and/or only to employees that require access to that system to perform their duties.
- 8.1.5. For further guidance, please refer to the [IT Acceptable Use Policy](#).

8.2. Passwords

- 8.2.1. You will be issued with unique passwords for accessing the Council's Systems. You must keep your password confidential and you should not disclose your password to anyone else.

APPENDIX 1

You must not write down your passwords or display them where they could be seen by others. You must take care to see that people do not see you entering your password.

- 8.2.2. It is the Council's policy that passwords should, be changed at regular intervals. During the course of your employment you are likely to be responsible for creating some of your own passwords. When creating a password, you should not select a password that can easily be guessed by others (e.g. the names of partner, children or pets). All employees must adhere to the [IT Corporate Password Policy](#).
- 8.2.3. When you have logged into any computer you should ensure that it is left securely so that no unauthorised person can access it. Whenever you leave your computer (whether working in a Council premises, at home or a third party premises), you must lock it by pressing 'Ctrl + Alt + Delete' and then confirming that you wish to lock your workstation, or by pressing 'Windows key (⊞) + L'.
- 8.2.4. If you have been issued with a portable device (mobile telephone, tablet etc.) this should be password/pin code protected and locked at all times when not in active use. You must not store the pin code with the device. When you leave your work area you should take the portable device(s) with you, or store away safely.
- 8.2.5. Personal or confidential data/information belonging to or held by or on behalf of the Council or its partners must not be stored on removable media, such as USB memory sticks, CDs or external hard drives without the express permission of IT Services. Where such data/information is permitted to be stored on a memory stick, it must be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused. For further information, please refer to the IT Acceptable Use Policy.

9. PERSONAL USE

- 9.1. The Council recognises that there are times when you may want to use its systems and equipment for non-work related purposes, and in recognising this need the Council permits you to use them for personal use.
- 9.2. You must not use the systems or equipment for personal use during working hours. If you work flexible hours/flexibly then personal use must be at a time outside of your work hours.
- 9.3. You must not allow personal use of equipment or systems to interfere with your day to day duties. Excessive non-job related use of the Council's equipment or systems during contractual hours may be subject to disciplinary action.
- 9.4. You must not store personal files on Council systems as there is a cost to the public purse for such storage and backup of the same.

10. THE COUNCIL'S RIGHTS AND OBLIGATIONS

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

11. CYBER SECURITY

- 11.1. The Council has comprehensive security and antivirus protection systems in place, which protect devices that connect to the council's network and keep thousands of spam emails and viruses from reaching Council mailboxes every month.
- 11.2. Only equipment or systems which have antivirus installed can be connected to the Council's network, unless written permission is obtained from a SUM of Digital Tameside or the AD of Digital Tameside.

11.3. Phishing

- 11.3.1. Phishing is a type of social engineering attack in which cyber criminals trick victims into handing over sensitive information or installing malware. E-mail is currently the most vulnerable method for phishing, malware and identity theft. If you receive an email from an unknown source, or containing content which looks suspicious you can report this directly from your Email client by right clicking on the email in the list and selecting 'Report as Malicious'
- 11.3.2. If you think you have clicked on a phishing email, or opened a suspicious attachment switch off your computer immediately and report this to IT services.

11.4. Malicious Software ('Malware')

- 11.4.1. Malware' is a collective term used for malicious software - viruses, worms, spyware, rootkits, botnets, ransomware etc. A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user and/or business data.
- 11.4.2. There are many potential sources of malware, including websites, social media, removable media such as USB memory sticks and CDs, email, and software or documents downloaded off the internet.
- 11.4.3. Employees are NOT permitted to plug in any unauthorised devices into their computer and/or the wider network. Only equipment corporately issued and/or approved by IT services is permitted; unless written permission is obtained from a SUM of Digital Tameside or the AD of Digital Tameside.
- 11.4.4. A malware infection can be incredibly costly for the Council and can often be time-consuming for all involved. This may be through the loss of data or access to IT systems, staff time to recover the systems, and/or the delay or loss of council data. Additionally, malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines from the Information Commissioner's Office (ICO). Malicious software is a constantly evolving threat and the Council therefore applies controls to protect our systems and information from all forms of malware.
- 11.4.5. Specifically, users are prohibited from:
 - Uninstalling and/or attempting to reconfigure anti-malware, updates, logging or other protective services on the Council's systems;
 - Negligently, intentionally or recklessly, introducing any form of malware;
 - Sharing login credentials with another user;

APPENDIX 1

- Using personal email accounts instead of a Council email account to conduct Council business, and/or forwarding emails from a Council email account to a personal account;
- Introducing data-interception, password detecting or similar software or devices to the Council's network;
- Seeking to gain unauthorised access to restricted areas of the Council's network;
- Accessing or attempt to access data where the user knows or ought to know that they should have not have access.
- Attaching any device or removable media (e.g. CD, memory stick) to Council equipment without submitting it to IT Services for virus checking.

11.4.6. Failure to adhere to the above could result in disciplinary action and if necessary, referral to the Police.

12. USE OF IT AT HOME OR OUT OF THE OFFICE

12.1. The provisions of this Policy apply equally when working on Council data or equipment whether working in a corporate office location or outside of Council premises.

12.2. The use of personally owned equipment to access or store council data is prohibited.

13. BACK UPS

13.1. It is vital that backup procedures are in place to maintain the availability, integrity and confidentiality of data. IT Services backup the corporate servers on a regular basis.

13.2. All employees must be aware that IT only back up information stored on the network (shared drives). Information stored on local (C:) drives or the desktop is not backed up and would not be able to be recovered if the equipment was lost, corrupted etc. Therefore, information stored on local drives should be kept to a minimum.

14. CONTRAVENTIONS OF THE POLICY

14.1. Employees should be aware that the Council Systems including the internal and external email system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.

15. DISCIPLINARY IMPLICATIONS

15.1. Breaches of this policy may result in disciplinary action up to and including dismissal and may also result in referral to any professional regulatory bodies. Breaches may also result in employees being prosecuted under Data Protection legislation and the Computer Misuse Act 1990, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.

16. PERSONAL DATA BREACH INCIDENTS

16.1. All breaches of this policy and all other personal data breach incidents, irrespective of scale, must be reported to the Information Governance Team (information.governance@tameside.gov.uk) within the first 24 hours of knowledge to allow

APPENDIX 1

for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.

16.2. Where a data breach is established to have occurred and there is a high risk of adversely affecting individuals' rights and freedoms, we are required to report to the Information Commissioners Office within 72 hours of first knowledge of the breach, without exception. Failure to report an incident to the Information Governance Team may result in disciplinary action being taken.

16.3. For further information regarding, refer to the [Personal Data Breach Reporting Procedure](#).

17. DEFINITIONS

17.1. The following terms are referenced throughout this document and are defined as follows:

Term	Definition
Cloud services / infrastructure	Cloud services include infrastructure, platforms or software hosted by third-party providers and made available through the internet.
Employee(s)	Includes all employees, Members of the Council, Committees, temporary staff, volunteers, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.
Equipment	Includes, but is not restricted to, the following <ul style="list-style-type: none"> • Servers • Laptop and desktop PCs • Mobile phones / Smartphones • Tablets • Printers / scanners • Personal Digital Assistants (PDA's) • Text pagers • Wireless technologies • Digital Cameras and other photographic or video recording equipment (CCTV cameras, body cameras, dash cams, drones etc.) • MP3 Players • Storage devices including, but not limited to, sim cards, flash memory cards, CDs, DVDs, magnetic tapes, portable hard drives and USB memory sticks.
Hybrid Working	Employees who have the ability to work from multiple locations. Usually accompanied by portable computing equipment, employees can utilise any work space at any given time (including their home, Council Workspaces, customer sites, Touch Down Points etc.)
Infrastructure	An encompassing term to cover all components required to enable IT operations. Includes but is not restricted to, the following <ul style="list-style-type: none"> • Hardware • Software • network resources • servers • computers

APPENDIX 1

Term	Definition
	<ul style="list-style-type: none"> • switches • Access Points
Legislation	<p>Includes but is not restricted to:</p> <ul style="list-style-type: none"> • The Computer Misuse Act (1990); • The Copyright, Designs and Patents Act (1988); • The Data Protection Act 2018; • The Freedom of Information Act 2000; • The General Data Protection Regulations (UK GDPR); • The Regulation of Investigatory Powers Act 2000.
Personal (Wi-Fi) Hotspot	A wireless internet access point provided by a smartphone.
Personal Data	<p>Is any personal data as defined by UK GDPR and the Data Protection Act 2018.</p> <p>It is defined in the Data Protection Act 2018 at s.3 (2) as “any information relating to an identified or identifiable living individual.”</p> <p>Broadly this means any information (relating to a living individual who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council.</p> <p>The UK GDPR provides a non-exhaustive list of identifiers, including:</p> <ul style="list-style-type: none"> • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). <p>Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person.</p> <p>The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.</p>
Protected Information	<p>Is any information which is:</p> <ul style="list-style-type: none"> • Personal / Special Category Data; or • Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.
Special Category Data	<p>This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of:</p> <ul style="list-style-type: none"> • Racial or ethnic origin

APPENDIX 1

Term	Definition
	<ul style="list-style-type: none">• political opinions / beliefs• religious or philosophical beliefs• trade union membership• genetic data• biometric data (where used for ID purposes)• health;• sex life; or• sexual orientation. <p>Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.</p>
VPN (Virtual Private Network)	Refers to a secure network connection that uses the internet to transmit data. It allows employees to access the Council network out of the office from a Council issued laptop.

DRAFT

This page is intentionally left blank



IT Acceptable Use Policy

DRAFT

Date: December 2023

Version: V1.2

Document Version Control

Document Version Control		
Version Number	Date	Approved by
1.0	May 2018	Audit Panel
1.1	September 2021	N/a – consultation draft to IT/IG working group
1.2*	December 2023	N/a – consultation draft to Information Governance Group

*Version 1.2 of this policy now incorporates and replaces the following policies:

- Access & Security Protocol
- Removable Media Protocol
- Mobile & Remote Working Protocol
- Email, Communications and Internet Acceptable use

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

Document Version Control	2
1. INTRODUCTION	4
2. PERSONAL USE	4
3. EMAIL USE	4
4. TELECOMMUNICATIONS USE	6
4.3. Mobile Phone Usage	7
5. INTERNET USE.....	8
6. HOME, REMOTE AND MOBILE WORKING	8
7. PASSWORD SECURITY	10
8. STAFF LEAVERS AND INTERNAL MOVERS	10
9. REMOVABLE MEDIA	11
10. ACCESS CONTROL.....	12
10.1. System Access	12
10.2. Network Access Control	12
10.3. Operating System Access Control.....	13
10.4. Application and Information Access.....	13
10.5. Supplier's Remote Access to the Council Network.....	13
11. COMPLIANCE	13
12. HARASSMENT AND ABUSE	14
13. DISCIPLINARY IMPLICATIONS.....	14
14. DEFINITIONS	15

1. INTRODUCTION

- 1.1. IT is an integral part of Tameside Metropolitan Borough Council's (the Council) activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council IT equipment and systems in the course of their duties. This policy is designed to enable the Council to:
- Get the best return possible for the investment it has made in technology;
 - Gain maximum benefit from email and the internet;
 - Comply with the law, in particular Data Protection Law;
 - Minimise legal and other risks associated with the use of technology;
 - Ensure effective running of the Council's business;
 - Minimise the risk of disruption caused by computer viruses and inappropriate use of IT; and
 - Provide clear information to employees and councillors and increase IT skills of our employees and residents.
- 1.2. This policy applies to Council employees, including temporary contact staff and volunteers, Councillors, agency workers, contractors, third parties and all partners who use the Council's technology.
- 1.3. Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of a Service Unit Manager of Digital Tameside or the Assistant Director of Digital Tameside.
- 1.4. In order to protect the Council's Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trade unions.

2. PERSONAL USE

- 2.1. The Council recognises that there are times when you may want to use its systems and equipment for non-work related purposes, and in recognising this need the Council permits you to use them for personal use.
- 2.2. You must not use the systems or equipment for personal use during working hours. If you work flexible hours/flexibly then personal use must be at a time outside of your work hours.
- 2.3. You must not allow personal use of equipment or systems to interfere with your day to day duties. Excessive non-job related use of the Council's equipment or systems during contractual hours may be subject to disciplinary action.
- 2.4. You must not store personal files on Council systems as there is a cost to the public purse for such storage and backup of the same.
- 2.5. When accessing the internet for non-work purposes you may only view web pages. You may not download files/documents because they contain a risk of contamination by malware. The Council's filtering system should prevent you from downloading programmes.

3. EMAIL USE

- 3.1. Employees are only permitted to use the email system for work purposes. Corporate email should not be used to send personal emails or send emails for party political purposes or promotion of personal financial interests.

APPENDIX 2

- 3.2. All emails may be subject to monitoring. All emails that you create should adhere to the provisions of this policy, and in particular comply with the requirements set out in this section.
- 3.3. Employees should treat e-mail communications with the same degree of care and professionalism as they would a letter sent out on company-headed notepaper. They should all meet 'the Chief Executive Test' namely would the Chief Executive send this email out on behalf of the Council, or more importantly would this e-mail give the Chief Executive cause for concern if they saw it? E-mails should be courteous and written in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour should be avoided, as it can be misinterpreted. The sending, or forwarding on, of jokes by e-mail (or as an attachment) is strictly prohibited.
- 3.4. The sending, or forwarding on, of curt, rude, sexually explicit, racially biased or offensive emails (or attachments) is strictly prohibited. Employees should not send unsolicited, irrelevant, or inappropriate e-mail messages internally or externally, nor should they participate in chain or pyramid letters by e-mail. Furthermore, personal opinions should not be presented as if they were those of the Council.
- 3.5. Council emails must not be forwarded on to a personal email account. Emails sent in these ways exit the Council's network and are transmitted over an untrusted network. If an email or attachment containing protected information is sent to a personal device/email account, the contents are open to misdirection, interception and corruption and therefore this would be in breach of this Policy.
- 3.6. You should not use the email system in breach of any of the Council's employment policies, particularly the Council's Equal Opportunities Policy, Bullying and Harassment Policy and Data Protection Policy. Employees must not use the e-mail system to send inappropriate messages or images via the email system (whether internally or externally). Inappropriate messages would include those, which are:
- Sexually explicit
 - Offensive (whether to the recipient or to a third party)
 - Potentially damaging to the Council's reputation and / or standards expected by the public
 - Defamatory or libellous
 - Discriminatory (e.g. racist or sexist)
 - Constitute harassment (see section 12)
- 3.7. Care should be taken when sending confidential, personal, or other sensitive information. Emails sent between two ".gov.uk" accounts are generally deemed to be safe and do not require additional encryption, though employees are directed to check the Council's [Safe to Send List](#) prior to sending any protected information. All emails containing protected information sent to non .gov.uk recipients must be sent using Egress secure Mail. Consideration should also be given to using password protection on attachments (even where sent through Egress) for particularly sensitive information, though use of encrypted email is the minimum standard to be used.
- 3.8. E-mail is a 'publication' for the purposes of the law. Any e-mail that includes information taken from another source (such as a publication or a website) may also breach copyright, for which the Council may be held responsible. Messages sent via the email system can give rise to legal action against the Council. Claims of defamation, harassment and breach of confidentiality or contract could arise from a misuse of the Systems. Email messages are disclosable in any legal action commenced against the Council relevant to the issues set out in the email. Employees should note that E-mail messages and any attachments can be used as evidence in many circumstances. They may have to be disclosed under the

APPENDIX 2

Freedom of Information Act 2000, or as part of a Subject Access Request under the Data Protection Act 2018 and UK GDPR.

- 3.9. The Council's email disclaimer and a corporate signature file including contact details are automatically added to emails sent from PCs/Laptops. This should not be removed. The corporate email disclaimer and corporate signature file are not automatically added to emails sent from a corporate smartphone.
- 3.10. As with other forms of business communications, you should retain copies of the emails you send, where necessary, for an appropriate length of time. Outlook automatically deletes emails after two years from the sent or received date in line with the Council's [corporate email deletion protocol](#). Any emails stored on a shared drive/SharePoint must only be retained as long as is necessary and in line with the Corporate Retention Schedule.
- 3.11. Employees should not use the email system for the storage of documents/attachments. This content will be automatically deleted after two years in-line with the [corporate email deletion protocol](#). Similarly, these documents are not available to others should an employee leave the Council.
- 3.12. If you send an email to an incorrect recipient, you should telephone the recipient immediately and ask them to 'double delete' (delete from their inbox and then delete again permanently from their deleted items folder) the email. You must also contact your immediate line manager and notify the Information Governance team by using the Information Security Incident Reporting Form which is contained in the [Personal Data Breach Reporting Procedure](#).
- 3.13. If an email message is sent to you in error, you should contact the sender immediately. If the email message contains confidential information you must not disclose or use that confidential information. If you receive an email of this nature you should contact your immediate line manager and double delete the email once the sender and your line manager are notified.
- 3.14. Autocomplete is an email feature that is enabled as standard. Autocomplete suggests email addresses in the To, cc or bcc fields when composing an email. These suggestions are based on the people you have previously emailed. It remains the responsibility of the individual to double check the suggested email address is correct. This feature can be disabled by the user.
- 3.15. You should only open emails with attachments from persons or organisations that you are familiar with. If you receive an email with an attachment from an unknown source and you are suspicious as to the nature of the communication you should report this to IT Services by using the 'Report as Malicious' button within your email.
- 3.16. If you receive an email with an attachment from a known source, or an email you are not expecting, you should contact the source by telephone in order to confirm that the email is genuine. You should not open any emails which do not appear to relate to Council business and seem to contain jokes, graphics or images as such emails regularly contain viruses.
- 3.17. Employees should take care when subscribing to email newsletters or marketing campaigns. High volumes of this type of email place a strain on the Council's storage and there is a cost to the public purse for storage and backup of those emails. Consideration should be given to unsubscribing where the newsletter is no longer required for work purposes and employees can also use the block sender function in Outlook.

4. TELECOMMUNICATIONS USE

APPENDIX 2

- 4.1. Employees are permitted to use the Council telephony system (including mobile phones) for personal calls. However, where a cost is incurred employees will be required to reimburse the Council for the full cost of the call. Excessive non-job related use of the Council's telephony system and/or mobile telephones may be subject to disciplinary action.
- 4.2. Employees must not use telecommunications systems and equipment provided by the Council for any activity that is illegal, for harassment or abuse of others, or for personal gain. Any employee found doing so may be subject to disciplinary action.
- 4.3. Mobile Phone Usage**
 - 4.3.1. Some employees will have use of a corporate mobile phone or a smartphone (if requested by the employee's manager based on an individual basis to support the delivery of service provision).
 - 4.3.2. Your corporate mobile phone may be used for personal use in accordance with section 2.
 - 4.3.3. Staff who are on the TMBC payroll may use their corporate mobile phone for personal calls and texts but this usage must be declared each month and paid via salary deduction via the "Mobile bills" function on the staff portal home page. Excess data usage (such as streaming video content) is prohibited as this cannot be declared and paid for.
 - 4.3.4. Staff who have been issued with a corporate mobile phone but who are not on the TMBC payroll (such as agency staff) may not use their device for personal usage as the cost for this cannot be quantified or recovered.
 - 4.3.5. The Council maintains a blacklist of apps that it does not authorise for business use and you will be prevented from downloading or accessing these on your corporate device.
 - 4.3.6. The Council's mobile phone provider implements an 18+ policy on your device which will prevent you from accessing inappropriate web pages. This includes pornography and illegal sites, as well as gambling, payday loan and racist sites. Employees are not permitted to use their corporate smartphone to access any site with inappropriate content. Employees may be subject to disciplinary action if they attempt to search for or access sites with inappropriate content. In exceptional cases, employees may need to access this type of site for work related purposes. If this need arises they must seek written authority to do so from the Assistant Director Digital Tameside, the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.
 - 4.3.7. To protect the Council's data that will be held on a corporate smartphone users must ensure the device is registered with the corporate security server/MDM. Details of how to do this will be sent to you when you first collect the device
 - 4.3.8. Where the Council provides a smartphone to an employee, it is the responsibility of the employee to ensure the security updates that are automatically deployed to devices are promptly downloaded. This is best achieved by ensuring automatic updates are set to "on" in the device Settings Menu. The device may prompt you to connect to a wifi network or to charge it before downloading an update. You should ensure this is performed at the very earliest opportunity.
 - 4.3.9. If your device is stolen or you lose or misplace it you must immediately notify IT Services via the IT Servicedesk. This is so that we can bar the device to ensure there is no further usage. You must also notify The Risk, Insurance and Information Governance Team by completing the [data breach form](#) so the incident can be investigated.
 - 4.3.10. Corporate mobile phones must be returned to IT Services when you leave or no longer require the use of it. Under no circumstances should you hand ownership over to another member of staff, this could constitute a data breach.

5. INTERNET USE

- 5.1. The internet may be used for legitimate business purposes or for personal use in accordance with section 2. Employees should be aware that all visits to websites on the Internet are logged and monitored by software operating on the Councils web server and may be subject to audit and inspection and disclosure under the Freedom of Information Act 2000.
- 5.2. You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council's Equal Opportunities Policy and / or the Council's Bullying and Harassment Policy
- 5.3. The Council has installed software to prevent access to inappropriate web pages. This includes pornography and illegal sites, as well as gambling, payday loan and racist sites. Employees are not permitted to access any site with inappropriate content and all internet activity is monitored, including any attempt to access or search for such sites. Employees may be subject to disciplinary action if they attempt to search for or access sites with inappropriate content. In exceptional cases, employees may need to access this type of site for work related purposes. If this need arises they must seek written authority to do so from the Assistant Director Digital Tameside, the Head of Risk Management and Audit Services or the Council's Monitoring Officer in advance.
- 5.4. It may, very rarely, happen that despite the protection systems, an employee accidentally visits an inappropriate site. If this happens then they must inform the Assistant Director Digital Tameside and the Head of Risk Management and Audit Services immediately by e-mail to avoid the possibility of being suspected of seeking to access inappropriate web pages and to enable ICT Services to block future visits.
- 5.5. Employees may use the internet to carry out their own private transactions (e.g. internet shopping) in their own time but you may not carry out transactions, which would be viewed as inappropriate under other parts of this Policy. Your Tameside email address is not to be used for private transactions. Please only use personal email addresses. The Council will not accept any responsibility for any loss that you may suffer as a result of personal use of the internet. Employees are reminded that the Council does monitor internet use.

6. HOME, REMOTE AND MOBILE WORKING

- 6.1. Post-Covid, many Council employees now access and process information outside of a traditional office setting. This Policy covers all locations where an employee may work, including a corporate office location, another business location or the home.
- 6.2. Employees who work from anywhere outside of the council network will need to register for Multi Factor Authentication (MFA) which is a mandatory additional level of security required to gain access into the council network.
- 6.3. All employees are responsible for the safety and security of portable devices issued to or used by them. Particular care must be taken when moving equipment between locations and storing when not in use.
- 6.4. Where the Council provides a laptop to an employee and this device is mainly used out of the office, it is the responsibility of the employee to ensure that the anti-virus updates and software updates that are automatically deployed to devices are promptly downloaded. This is achieved by regularly connecting to the network via VPN then selecting "shut down" and waiting until the process is complete before closing the device.

APPENDIX 2

- 6.5. Employees must take additional care when working at home to ensure that any 'Smart Home' or 'Internet of Things (IOT)' devices are not able to connect to the Council's IT equipment. Particular care should be taken around 'smart speakers' and / or 'smart assistants' (including but not limited to Amazon Alexa, Google Assistant, Siri etc.) built into devices including an employee's personal smartphone or tablet as such devices are capable of recording conversation that they pick even when they appear inactive.
- 6.6. All protected information (including information stored on portable devices and in paper files, including printed and handwritten documents and notes) must not be left unattended or where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight. Unauthorised disclosure of protected information is a breach of this Policy and the law.
- 6.7. Where Council equipment and protected information is used at home this must be kept safely and securely at all times. Employees must :
- ensure that only they have access to the equipment/information;
 - ensure that the equipment/information is safely and securely locked away when not being used;
 - prevent access to the Council equipment and data/information, by family members and visitors;
 - ensure that any telephone conversations discussing protected information cannot be overheard.
- 6.8. Employees who work at home must have a suitable workstation where possible and the above issues must be considered.
- 6.9. Printed documents and/or handwritten notes which contain protected information must be disposed of appropriately. When working from a remote location (including at home), it is expected that any such paperwork is kept concealed at a minimum, and where possible is stored in a lockable cupboard or drawer, until you are able to make arrangements to securely dispose of paperwork at a Council office location. All waste paper which contains protected information must be disposed of appropriately in a Council office location by placing into the locked confidential waste bins. Under no circumstances should paperwork containing protected information be thrown away in domestic recycling or waste bins. For further information on the secure disposal of information see the Retention and Disposal Guidelines/Schedule.
- 6.10. Employees must be aware of their surroundings and take appropriate measures when viewing information on a portable device to ensure it is not within view of others. This applies whether working at home or in a public space.
- 6.11. When working out of the office, employees should avoid using Wi-Fi Hotspots or free Wi-Fi connections provided by retail outlets, coffee shops etc. Even when connected via the Council's VPN, hackers could still intercept transmissions potentially revealing protected information or password and login details. Individuals are required to assess the risks based on the data they work with. Those that work with personal and sensitive data should not use such facilities and instead use the personal Wi-Fi hotspot facility on their Council provided smartphone (also using the VPN software on their laptop). Others are permitted to use these facilities but must never give any information about their Council email account or passwords. Employees must refer to their manager or the Risk, Insurance and Information Governance Team if they are uncertain. The only exception to this would be a private network that requires a password to access, for example Wi-Fi at another Local Authority building, or at a business or academic premises. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.

APPENDIX 2

- 6.12. Portable devices issued by the Council are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover.
- 6.13. Employees must seek advice from the following services before taking any Council owned portable device outside of the United Kingdom:
- Risk and Insurance Team
 - The device may not be covered by the Council's normal insurance against loss or theft;
 - There is also the possibility that the device may be confiscated by Airport Security staff, which could result in having to leave them behind, or they may request to see the contents, which could result in a breach of this policy and possibly the law if the device contains protected information.
 - ICT Services (via the IT Service Desk)
 - Activity and logins to TMBC accounts from abroad are logged and investigated to ensure they do not relate to suspicious cyber criminal activity;
 - To ensure appropriate data roaming packages are included for smartphones to protect against excess charges and to make the users are aware of the additional costs
- 6.14. Employee's that work remotely should be based in the UK. If anyone has a requirement to work for a period of time outside the UK, this must be discussed with your manager and HR will need to authorise this.

7. PASSWORD SECURITY

- 7.1. Passwords are the first line of defence for the Council's IT systems and together with unique user ID's, passwords help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of the Council's computers and systems.
- 7.2. In using the IT equipment provided to you by the Council you accept that you have read and accept the details within this policy, the [IT Security Policy](#) and the [IT Corporate Password Policy](#).

8. STAFF LEAVERS AND INTERNAL MOVERS

- 8.1. Where an employee leaves the Council, the manager must follow the Leavers Checklist available via the intranet and must also log a "leaver request" through the IT Service Desk to ensure the correct system accesses are removed and the return of all equipment is arranged on the leaver's final working day.
- 8.2. Where employees move internally between different service areas within the Council, the manager of the team being left has responsibility for notifying IT Services. The manager must follow the Movers Checklist available via the intranet and must also log a 'movers request' through the IT Service Desk. Logging a ticket will ensure
- that IT equipment can be changed where necessary
 - the employee's systems and data access can be amended as appropriate.

APPENDIX 2

- the manager is aware of their responsibility to make their employee aware of the need to remove all data pertaining to their previous job role (emails, documents etc.)
 - the employee is copied into the ticket and informed of their responsibilities around purging emails, files, data pertaining to their old role
- 8.3. The manager of the new team will log a “new starter” ticket on the IT Service Desk. The new starter ticket will ensure
- the appropriate IT equipment needed for their new employee is provided
 - the appropriate system access is granted
- 8.4. Any access permissions for the new job role must be obtained in line with the process outlined in Section 10.
- 8.5. If an employee is deemed to have contravened this policy or any other policy on the [Data Protection/Information Governance Framework](#), potentially jeopardising the availability, confidentiality or integrity of any systems or data/information, their access rights to the system or data/information will be suspended pending further review.

9. REMOVABLE MEDIA

- 9.1. Only by exception and where there is a valid business need, as agreed by the employees Service Unit Manager and with approval from a SUM of IT Services will permission be granted to store data/information on removable media (USB memory sticks, CDs, external hard drives). In all instances the device must be purchased by IT Services via the Council’s approved purchasing system and will be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused.
- 9.2. Removable media must not be used as the sole storage method for business data/information. All data/information must be stored on the Council’s infrastructure which is secure and appropriately backed up.
- 9.3. Removable media must not be used to store backup data. All data held on the Council’s infrastructure is already appropriately backed up.
- 9.4. Any employee who has access to or use of removable media is responsible for the safety and security of the media and the data/information stored on them and must ensure they are not compromised whilst under their control.
- 9.5. Employees should be aware that the use of removable media on the Council’s network is logged and monitored and may be subject to audit and inspection.
- 9.6. Any removable media connected to the Council’s network that is not encrypted will be ‘read only’ and no information will be able to be saved onto it. A message will be displayed by the monitoring software. Employees will still be able to view the contents of non-encrypted media.
- 9.7. Files on removable media are automatically scanned for viruses before opening.
- 9.8. Removable media issued by the Council must only be used for the purposes of Council business. Employees must therefore ensure that any removable media is not accessed by anyone outside the Council.

APPENDIX 2

- 9.9. Use of encrypted removable media to transport or access protected information outside of the Council's network should be minimised and used as a last resort when no other method of accessing information is available. Employees must be able to demonstrate that reasonable care is taken during transportation to avoid damage to or loss of the physical device or data held on it.
- 9.10. Where there is an approved Information Sharing Agreement or Processing Agreement in place that allows a third party access to Council information, the third party is required to follow this Policy if they use removable media for the purpose of holding or transferring information. It is the responsibility of the service who share the data to ensure this Policy is followed.
- 9.11. Council issued removable media must not be connected to non-Council owned equipment.
- 9.12. Passwords needed to access protected information on removable media must only be disclosed to those authorised to access the information held on the media. Passwords must never be written down or stored alongside the media.
- 9.13. In order to minimise physical risk such as loss or theft, all removable media must be stored in an appropriately secure and safe environment when not in use (e.g. locked cupboard or drawer).
- 9.14. Any incident where protected information is lost, damaged (physical damage to the removable media or deletion of the data upon it), leaked or put at risk must be reported as a potential data breach incident. It is the responsibility of all employees to immediately report any actual or suspected breaches in information security by informing their line manager and the Information Governance Team (information.governance@tameside.gov.uk). Failure to report any actual or suspected breach could result in an incident having more serious consequences than would otherwise have been the case and could result referral to and sanction by the Information Commissioner's Office (ICO).
- 9.15. All removable media devices (see definitions) should be returned to IT Services to securely delete/destroy the data and to dispose of or reallocate the removable media. This is essential to minimise the risk of the accidental disclosure of sensitive information.
- 9.16. For further details please refer to the [IT Security Policy](#).

10. ACCESS CONTROL

10.1. System Access

- 10.1.1. Each user will be allocated access rights and permissions to computer systems and data that:
- Are appropriate for the tasks they are expected to perform;
 - Have a unique login that is not shared with or disclosed to any other user;
 - Have an associated unique password that complies with the Council's password guidance.
- 10.1.2. Where appropriate, multi-factor authentication (MFA) and/or single sign-on will be required to access Council systems.
- 10.1.3. System owners must review user access rights at regular intervals to ensure that the appropriate rights are only allocated to present employees of the service area and/or only to employees that require access to that system to perform their duties. System administration

accounts must only be provided to users that are required to perform system administration tasks.

10.2. Network Access Control

10.2.1. Employees are not permitted to plug in any unauthorised devices into their computer and/or the wider network. Only equipment corporately issued and/or approved by IT services is permitted; unless written permission is obtained from a SUM of Digital Tameside or the AD of Digital Tameside.

10.3. Operating System Access Control

10.3.1. Access to operating systems is controlled by a secure login process. The access control defined within this policy must be applied. The login procedure must also be protected by:

- limiting the number of unsuccessful attempts and locking the account if exceeded
- the password characters being hidden by symbols.

10.3.2. All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).

10.3.3. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

10.4. Application and Information Access

10.4.1. Access within software applications must be restricted using the security features built into the individual product. The manager of the software application is responsible for granting access to the information within the system. The access must be:

- separated into clearly defined roles
- the appropriate level of access required for the role of the user
- unable to be overridden (with the admin settings removed or hidden from the user)
- free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access
- logged and auditable

10.5. Supplier's Remote Access to the Council Network

10.5.1. Partner agencies or Third party suppliers must not be given access to, or provided access instructions for the Council's network or any of its systems without permission from IT within a business case. Any proposed new access to the network or any system operated by the Council must be reviewed under the DPIA process, with input from Risk Management and Audit Services and the Information Governance Team. Any changes to a supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by IT Services with assurances from the SIRO.

10.5.2. All partner agencies or third party suppliers seeking to remotely access the Council's network must, upon receiving authorisation from IT, use the remote access portal.

10.5.3. Partners or Third party suppliers must contact IT before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

11. COMPLIANCE

- 11.1. This Policy takes into consideration all applicable statutory, regulatory and contractual security requirements.
- 11.2. All breaches of this policy and all other personal data breach incidents, irrespective of scale, must be reported to information.governance@tameside.gov.uk within the first 24 hours of knowledge to allow for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.
- 11.3. Where a data breach is established to have occurred and there is a high risk of adversely affecting individuals' rights and freedoms, we are required to report to the Information Commissioners Office within 72 hours of first knowledge of the breach, without exception. Failure to report an incident to the Information Governance Team may result in disciplinary action being taken.
- 11.4. For further information regarding, refer to the [Personal Data Breach Reporting Procedure](#).
- 11.5. It is the responsibility of all employees to ensure that they have read and comply with the conditions laid out in this protocol.
- 11.6. Non-compliance with this protocol could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.
- 11.7. If any user is found to have breached this protocol, they may be subject to the Council's Disciplinary Procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
- 11.8. If you do not understand the implications of this protocol or how it may apply to you, please contact the information Governance Team (information.governance@tameside.gov.uk) or the Council's Information Security Officer (cybersecurity@tameside.gov.uk).

12. HARASSMENT AND ABUSE

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

13. DISCIPLINARY IMPLICATIONS

- 13.1. Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being personally prosecuted under the Computer Misuse Act 1990,

APPENDIX 2

Data Protection Act 2018/UK GDPR or other applicable legislation and may also lead to prosecution of the Council, fines and/or civil claims for damages.

- 13.2. Misuse of Council owned IT equipment or software may also be a breach of the statutory Code of Conduct for Councillors, or other regulatory codes of conduct for professional occupations (Social workers, Solicitors etc.). Breaches of this policy may be reported to the relevant regulatory body.

14. DEFINITIONS

- 14.1. The following terms are referenced throughout this document and are defined as follows:

Term	Definition
Employee(s)	Includes all employees, Members of the Council, Committees, temporary staff, volunteers, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.
Equipment	Includes, but is not restricted to, the following: <ul style="list-style-type: none"> • Servers • Laptop and desktop PCs • Mobile phones / Smartphones • Tablets • Printers / scanners • Personal Digital Assistants (PDA's) • Text pagers • Wireless technologies • Digital Cameras and other photographic or video recording equipment (CCTV cameras, body cameras, dash cams, drones etc.) • MP3 Players
Personal Data	<p>Is any personal data as defined by UK GDPR and the Data Protection Act 2018.</p> <p>It is defined in the Data Protection Act 2018 at s.3 (2) as “any information relating to an identified or identifiable living individual.”</p> <p>Broadly this means any information (relating to a living individual) who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council.</p> <p>The UK GDPR provides a non-exhaustive list of identifiers, including:</p> <ul style="list-style-type: none"> • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses).

APPENDIX 2

Term	Definition
	<p>Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person.</p> <p>The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.</p>
Protected Information	<p>Is any information which is:</p> <ul style="list-style-type: none"> • Personal / Special Category Data; or • Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.
Removable Media	<p>Storage devices including, but not limited to, USB memory sticks, CDs, DVDs, SIM cards, memory cards, magnetic tapes, external/portable hard drives, solid state drives, digital cameras and / or other video recording equipment</p>
Special Category Data	<p>This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • political opinions / beliefs • religious or philosophical beliefs • trade union membership • genetic data • biometric data (where used for ID purposes) • health; • sex life; or • sexual orientation. <p>Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.</p>



**Social Media Use: Responsible
Conduct Policy**

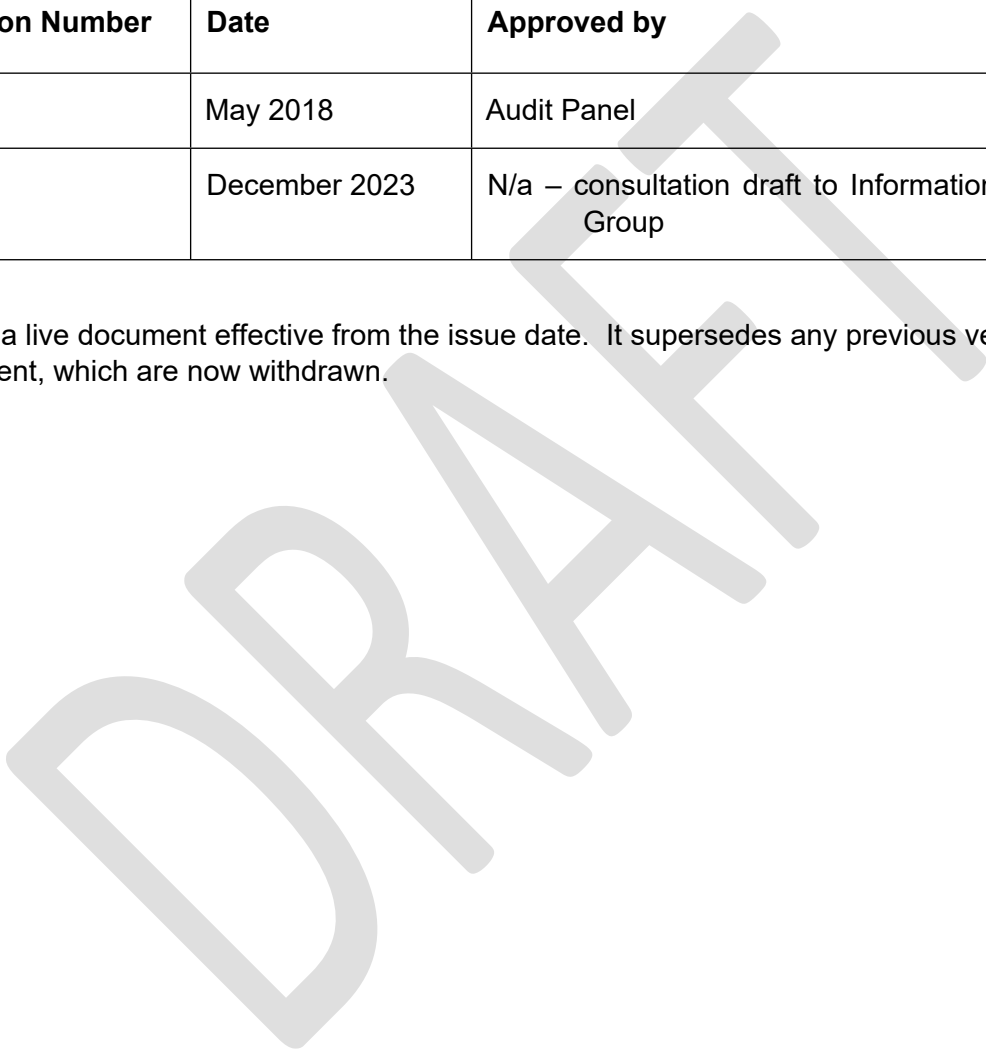
Date: December 2023

Version: V2.0

Document Version Control

Document Version Control		
Version Number	Date	Approved by
1.0	May 2018	Audit Panel
1.2	December 2023	N/a – consultation draft to Information Governance Group

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.



Contents

- Document Version Control**.....4
- 1. INTRODUCTION6
- 2. WHAT IS SOCIAL MEDIA?6
- 3. RISKS OF SOCIAL MEDIA.....6
- 4. WHAT ARE THE BENEFITS OF USING SOCIAL MEDIA?6
- 5. CONDUCT7
 - 5.10. Personal use of social media at work.....8
 - 5.11. Monitoring of online access at work.....9
 - 5.12. Inappropriate Posting9
 - 5.13. Disciplinary Implications.....9
- 6. GUIDANCE FOR EMPLOYEES9
- 7. GUIDANCE FOR MANAGERS.....10
- 8. FINALLY.....10

DRAFT

APPENDIX 3

1. INTRODUCTION

- 1.1. All Council employees (including full and part-time employees, Councillors, temporary or agency workers, consultants and volunteers) are in a public role and accordingly are under close scrutiny. As such, particular care has to be taken when engaging with social media to ensure that employees maintain appropriate standards and do not bring the Council or its activities into disrepute.
- 1.2. This policy applies to both work related and personal social media activity and is to be read in conjunction with other policies on the [Data Protection/Information Governance Framework](#).
- 1.3. Content is not limited to text, it also includes images and videos.

2. WHAT IS SOCIAL MEDIA?

- 2.1. Examples of social media include, but are not limited to, Facebook, X (Formerly known as Twitter), Reddit, blogs, YouTube, Instagram, TikTok, Tumblr, Wikipedia, Snapchat and networking sites such as LinkedIn. The term covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations. This also includes, but is not limited to, messaging platforms such as Facebook Messenger and WhatsApp.
- 2.2. This policy applies to, but is not limited to, the following content:
 - All blogs, wikis, forums, and social networks hosted or sponsored by the Council;
 - Any personal blogs that contain postings about the Council's business, councillors, employees, residents, customers, or partners including the local police;
 - Any postings about the Council's business, councillors, employees, residents, customers, or partners and local police, on any external blogs, wikis, discussion forums, social networking sites, or messaging apps ; and
 - Participation in any video related to the Council's business, councillors, employees, residents, customers, or partners; whether you create a video to post or link to on your blog, you contribute content for a video, or you appear in a video created either by another Council employee or by a third party.

3. RISKS OF SOCIAL MEDIA

- 3.1.1. Employees are reminded to be security conscious when using social media. Social media allows people to post detailed personal information, which can form the basis of security questions and passwords, and may pose a risk to the security of Council systems and individuals themselves.
- 3.1.2. Information can be obtained through social media from information placed into a user's profile and settings, direct postings put up by the user, or are often obtained by malicious third parties through innocent looking surveys that are commonly shared amongst social media users which allow them to obtain a wealth of personal information.

4. WHAT ARE THE BENEFITS OF USING SOCIAL MEDIA?

- 4.1. Used carefully, social media can bring people together over common interests, can be useful for communicating with a wider audience and allows our residents to initiate and participate in a dialogue with us as a Council. However, you must treat social media with

APPENDIX 3

respect and always remember that any information or comments you publish on any site (internal or external):

- May stay public for a long time, and even if deleted, may still be available within a public archive;
- Can be quickly disseminated and control over such information can be rapidly lost;
- Can be republished / shared on other websites;
- Can be copied, used and amended by others;
- Can be changed to misrepresent what you said; and
- Can attract comments and interest from other people / the media.

4.2. We expect all employees to be aware of, and comply with, the standards, conditions of use and guidelines for posting, laid down by the owner of any social media or messaging site or network.

5. CONDUCT

5.1. This policy applies to all employees, including temporary contract staff, agency staff, volunteers, contractual third parties, Councillors, committees and agents of the Council. Hereafter any reference to employees is intended to cover all of the above.

5.2. Whether your use of social media is for business or personal use, what you say could have an influence on your ability to conduct your job responsibilities, your work colleagues' abilities to do their jobs, and the Council's business interests and reputation.

5.3. All employees should consider carefully whether they wish to include their employment with the Council on any personal profile. All employees are expected to behave appropriately when using social media, and in ways that are consistent with the Council's values and policies.

5.4. This guidance note sets out the principles which Council employees are expected to follow when using social media and gives interpretations for current forms of interactivity. Social media is a fast moving environment and it is impossible to cover all circumstances. However, the principles set out in this document must always be followed.

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

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

5.7. To this end employees should not:

- Engage in activities on social media that might bring the Council into disrepute or damage the public's trust and confidence in the Council and / or the employee's fitness to undertake their role;
- Conduct themselves in a way that is detrimental to the Council and / or fellow employees;
- 'Speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council), or post opinions on behalf of the Council, unless you are specifically authorised to do so in writing. If you have not been authorised, then please speak to your line manager before taking any action;

APPENDIX 3

- Use Social media in any way to send, post, 'like' or share abusive, offensive, hateful, libellous or defamatory content (which includes, but is not limited to, messages/text, pictures, video, audio recordings), especially those which concern members of the public, councillors, customers / service users, employees, agency staff, consultants or the Council as an entity;
 - Use Social Media in any way to send, post, 'like', comment on or share messages or pictures created by about customers or service users unless you have their express written consent;
 - Post confidential, or any other information or content that could constitute a breach of copyright or data protection legislation. Examples include;
 - Taking an image from the Internet and using it on Facebook
 - Taking Images of items belonging to service users and posting them on Social media regardless of intention, should that item allow others to identify them.
 - Taking images of good examples of service users or groups good work without seeking consent
 - Posting images of fly tipping that contain personal information.
 - Use their personal email addresses for official Council business;
 - Use the Council's social media for party political purposes or for the promotion of personal financial interests;
 - Participate in any personal blogging activities where you have indicated you are an employee of the Council, as your comments could be interpreted as the opinion or view of the Council, without prior management authorisation and appropriate disclaimers ("The views expressed here are my own and do not necessarily represent the views of Tameside Borough Council").
- 5.8. Should any employee believe they may have breached this policy, they must immediately raise it with their line manager.
- 5.9. Individuals in politically restricted posts (usually over salary scale point 38 / grade I+), those that provide regular advice and support to committees, Groups and panels or speak with the press and those that work in politically sensitive areas should not be seen to support any political party or cause. Any online activities associated with work for the Council should be discussed and approved in advance by a senior council manager.
- 5.10. **Use of Social Media for investigations**
Information gathered from social media can be useful when conducting investigations, **but** any investigations must be necessary for a specific and legitimate objective, proportionate to the objective in question, and carried out in accordance with the law, including the Human Rights Act 1998 ("HRA 1998"), European Convention on Human Rights ("ECHR"), Data Protection Legislation (DPA 2018, UK GDPR etc.) and Regulations of Investigatory Powers Act 2000 ("RIPA 2000").
6. Employees must read the Social Media Investigations/Internet Research Policy and [RIPA policies](#) before carrying out any research or investigations.
7. Any social media or internet research enquiries carried out under the Social Media Investigations/Internet Research Policy must be **attributable, overt, initial non-repeated research**. Any research which is covert, likely to reveal private information and is carried out or repeated with some regularity over a period of time will fall under the Council's [RIPA policies](#) instead. Employees must be aware that repeated viewing (2 or more times) of "open source" information requires RIPA authorisation.
8. Any employee who carries out social media investigation or internet research which breaches either policy will be subject to disciplinary action.

8.1. **Personal use of social media at work**

- 8.1.1. The Council recognises that there are times when you may want to use the IT Systems for non-work related purposes, and the Council permits you to use the IT Systems to access your personal social media. However, this should not be during working hours. If you work flexible hours/flexibly then personal use must be at a time outside of your work hours. The expectation is that use is not excessive as the primary purpose of the IT system is for work purposes. You must not allow personal use of the IT Systems to interfere with your day-to-day duties or the duties of your colleagues.
- 8.1.2. If you access personal social media sites whilst using a work computer, any transaction may be recorded as a Tameside Council IP address. That means it may look as if the Council itself has made the social media entry, or changes to an entry, and imply that the entry or opinion contained within is the opinion of the Council.
- 8.1.3. There is no unconditional right for an Employee to access such sites and the Council reserves the right to restrict access to social media (or certain websites) for particular employees if there is cause for concern over their use.

8.2. **Monitoring of online access at work**

- 8.2.1. You should note that, the Council monitors social media use in accordance with the provisions set down in the IT Security Policy [Link needed] and the Email, Communications and Internet Acceptable Use Policy [Link Needed], and unacceptable levels of use could lead to disciplinary action.

8.3. **Inappropriate Posting**

- 8.3.1. If an employee is found to have posted inappropriate material in any format on social media, they are expected to remove such material swiftly. If an employee refuses to remove it, they will automatically face disciplinary action. However, even where such material is removed in a timely manner, the employee may still face disciplinary action.

8.4. **Disciplinary Implications**

- 8.4.1. If the Council finds that an employee's social media use is not in accordance with the Council's policies and guidance, The following actions can be considered:-
- access to social media sites at work may be withdrawn
 - Removal of the right to work remotely
 - Disciplinary Action - if deemed sufficiently serious, this could result in dismissal.
- 8.4.2. Misuse of social media can also open employees up to criminal prosecution, which could result in others taking out a civil action against you, imprisonment and / or a fine.

9. **GUIDANCE FOR EMPLOYEES**

- 9.1. If you receive any media requests about something posted online, take their contact details and immediately advise your manager who will liaise with the Council's Policy, Performance and Communications Team. Do not engage in any communication with the media without authorisation from the Council.
- 9.2. Make sure all video, photographs and other media is safe to share, does not contain any confidential or derogatory information, and is not protected by any copyright or intellectual property rights. You must ensure that you have the required written permission from the providers and every person that appears on any video, photographs and other media that we use / share.

APPENDIX 3

- 9.3. If the content is official Tameside Council content then it must be labelled and tagged as such.
- 9.4. Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: "This is my personal work and does not necessarily reflect the views of Tameside Metropolitan Borough Council." Please note that a disclaimer will not protect you from potential disciplinary action should concerns be raised or reported.

10. GUIDANCE FOR MANAGERS


- 10.1. Please make sure you and your employees (including agency workers and contractors) are aware of and working within these guidelines. Please speak to the Assistant Director of Policy, Performance and Communications, the Information Governance Team, if you have any questions or concerns about interpreting this policy.
- 10.2. Managers are responsible for deciding what is appropriate, bearing in mind concerns about impartiality, confidentiality, conflicts of interest or commercial sensitivity.
- 10.3. If you, as a manager, believe any employee is breaching these guidelines or is spending too much time on social media, it may be appropriate to implement monitoring for that employee. If monitoring is required, contact Human Resources with your concerns and if agreed, contact IT to start the Monitoring. It is every manager's responsibility to ensure their employees (including agency workers and consultants) are not abusing Council IT facilities.

11. FINALLY....

- 11.1. These guidelines are to protect you and the reputation of the Council. They are not meant to restrict your genuine and work related use of what is an important method of communication and engagement. By its nature though, social media is fast and responsive, so when a mistake is made it can rapidly get out of control.
- 11.2. If you think social media may help your service you should contact the of Policy, Performance and Communications Team, who can support you and ensure your proposal is supported by the other work being done as part of the corporate communications strategy.

Agenda Item 8.

Report to:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Carol McDonnell – Head of Assurance
Subject:	INTERNAL AUDIT PLAN 2024/25
Report Summary:	This report presents the Audit Plan for 2024/25 along with the Audit Charter and Quality assurance & Improvement Programme.
Recommendations:	<ol style="list-style-type: none">1. Members approve the Draft Internal Audit Strategy and Plan for 2024/25 shown at Appendix 1.2. Members approve the Audit Charter for 2024/25 shown at Appendix 2.3. Members approve the Quality Assurance and Improvement Programme for 2024/25 shown at Appendix 3.
Corporate Plan:	The Internal Audit Plan provides assurance to the Audit Panel that the risks associated with the delivery of the Corporate Plan are being managed.
Policy Implications:	An effective risk based Internal Audit Plan provides assurance that the Council's policy framework is sufficient and operating effectively.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	There are no financial implications directly associated with this report.
Legal Implications: (Authorised by the Borough Solicitor)	<p>A properly functioning Internal Audit supports the Director of Resources (Section 151) in discharging their statutory responsibilities under:</p> <ul style="list-style-type: none">• S151 of the Local Government Act 1972 – to ensure the proper administration of financial affairs.• Section 114 of the Local Government Act 1988 – to ensure the Council's expenditure is lawful.• The Accounts and Audit Regulations 2015 – the Council must undertake an adequate and effective Internal Audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal audit standards or guidance.
Risk Management:	Delivery of a risk-based audit plan gives assurance to senior management and the Audit Panel that the Council's most significant / material risks are being managed.
Background Information:	The background papers can be obtained from the author of the report, Carol McDonnell, Head of Assurance:

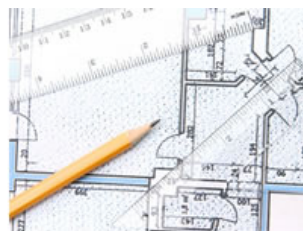
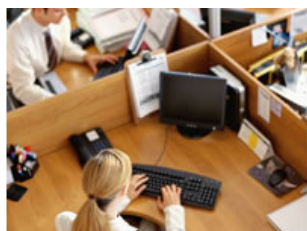
 0161 342 3231

 carol.mcdonnell@tameside.gov.uk

This page is intentionally left blank

ASSURANCE SERVICE INTERNAL AUDIT STRATEGY AND PLAN 2024/25

Page 109



MARCH 2024

1. INTRODUCTION

1.1 The purpose of this document is to present the proposed Internal Audit Strategy and Plan for 2024/25 to the Audit Panel for review and approval.

2. INTRODUCTION

2.1 This document summarises the results of Internal Audit's planning work, and sets out:

- Requirements of the Public Sector Internal Audit Standards
- Responsibilities
- The Planning Process
- Resourcing of Internal Audit and Counter Fraud
- Proposed Programme of Work for 2024/25 (the Audit Plan)
- Collaboration Arrangements
- Arrangements for Reporting Internal Audit Work

2.2 The plan has been prepared in accordance with the Public Sector Internal Audit Standards (PSIAS) and the Audit Charter, presented alongside this Strategy and Plan.

3. PUBLIC SECTOR INTERNAL AUDIT STANDARDS (PSIAS)

3.1 Standards for Internal Audit in local government are set out in the PSIAS and a Local Government Application Note from the Chartered Institute of Public Finance and Accountancy (CIPFA). The PSIAS represent mandatory best practice for all internal audit service providers in the public sector.

3.2 The PSIAS section '2010 Planning' states:

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals.

To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organisation's strategies, key business objectives, associated risks and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programmes, systems, and controls.

4. RESPONSIBILITIES

Internal Audit

4.1 The Internal Audit function is responsible for:

- Reviewing and developing the Council's governance processes, including:
 - Promoting appropriate ethics and values within the Council
 - Supporting effective organisational performance management and accountability
 - Communicating risk and control information to appropriate areas of the organisation
 - Coordinating the activities of, and communicating information among, the Audit Panel, External Audit, and management
- Evaluating the effectiveness of the Council's risk management processes and contributing to their improvement.
- Assisting in the maintenance and development of an effective control environment by providing robust independent assurance over its operation.

Management

4.2 Management is responsible for the establishment and maintenance of adequate control systems and ensuring that recommendations for improvement are implemented effectively in a timely manner.

Audit Panel

4.3 The Audit Panel is responsible for:

- Approving, but not directing, Internal Audit's Strategy and Audit Plan.
- Monitoring the performance of Internal Audit.
- Reviewing Internal Audit outcomes and seeking assurance that action has been taken where necessary.
- Receiving and considering the Head of Assurance's annual report.

Fraud Prevention and Detection

4.4 The primary responsibility for the prevention and detection of fraud rests with management. Management should report all irregularities in line with the Council's Counter Fraud Policy and Strategy.

4.5 It is not the role or responsibility of Internal Audit to detect fraud. However, Internal Audit will evaluate the potential for the occurrence of fraud in audit assignments, and review how the Council manages the risk of fraud.

4.6 The Counter Fraud Team will risk assess and investigate allegations and referrals, and complete proactive work to prevent and detect fraud.

5. THE PLANNING PROCESS

5.1 As part of the planning process, it is important to ensure that resources are effectively focussed, and the planning process has included reference to:

- Strategic Risk Register;
- Corporate Plan Priorities;
- Senior management's views on risk in their areas of responsibility;
- Key systems where there is materiality due to high financial value or number of transactions;
- Known previous areas of weakness;
- Areas affected by significant change in structure, legislation, system or process;
- Areas that relate to the savings programme and planned efficiencies; and
- National and local intelligence with audit colleagues, regulatory and professional bodies.

5.2 It is important for consultation to take place on the Audit Plan. Consultation has taken place with the following:

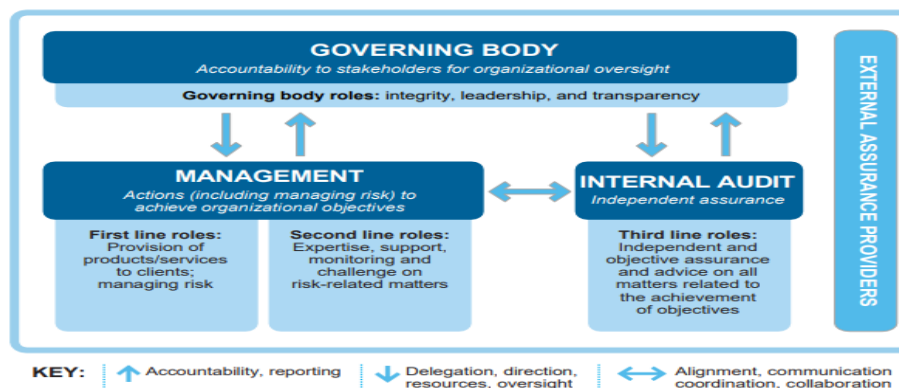
- Directors
- Chief Executive
- GMPF Assistant Directors
- Assistant Directors Delivery Group
- Single Leadership Team
- External Audit
- Chair of the Audit Panel

5.3 The Audit Plan is based on the Institute of Internal Auditors (IIA) three lines model of assurance.

5.4 This model ensures focus on key risk when developing plans.

5.5 Internal Audit seeks to identify assurances provided through the first and second lines and select the most appropriate method of obtaining assurance to support the Head of Assurance's annual opinion. This also aligns to the Council's approach to Risk Management.

The IIA's Three Lines Model

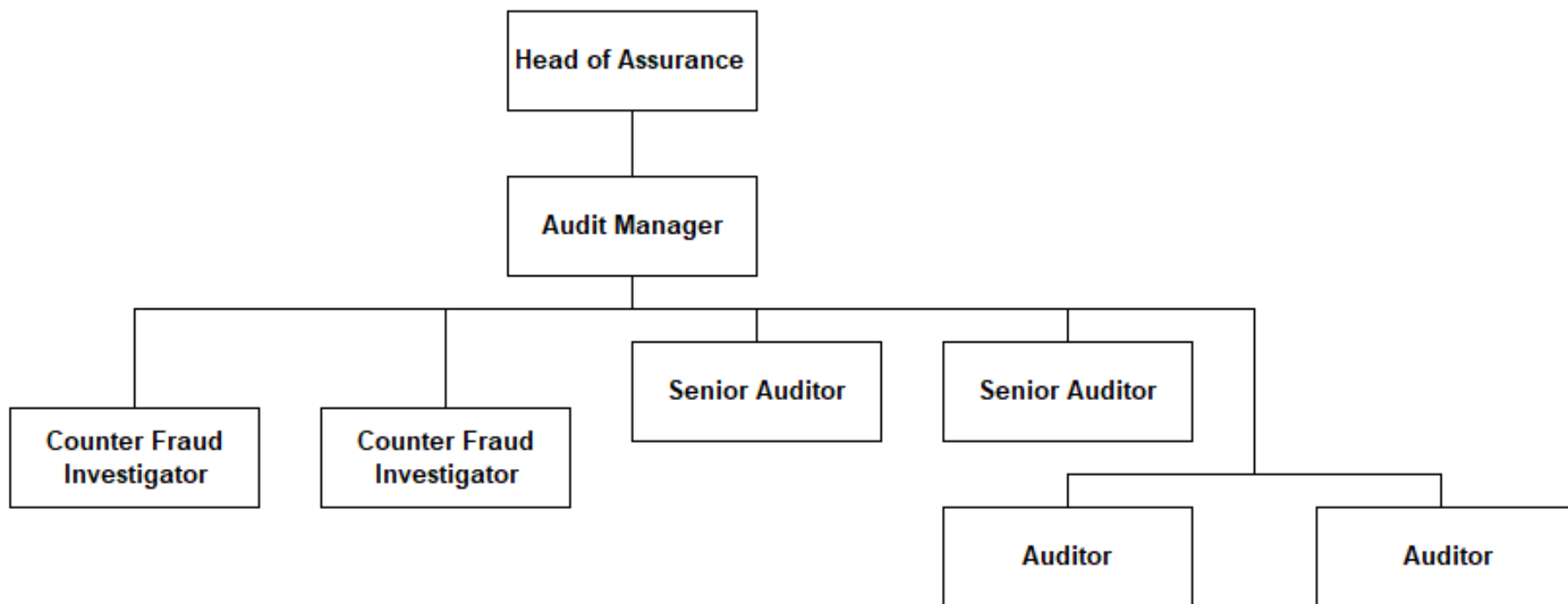


6. RESOURCING OF INTERNAL AUDIT AND COUNTER FRAUD

6.1 Internal Audit forms part of the wider Assurance Service, which is led by the Head of Assurance. The Assurance Service includes the following areas:

- Internal Audit and Counter Fraud
- Risk, Insurance, and Information Governance
- National Anti-Fraud Network (NAFN)

6.2 The current structure of the Internal Audit and Counter Fraud is:



6.3 For the completion of Internal Audit assignments, the resources available are outlined overleaf:

Post	Available Days	Overheads	Management	Carry Forward	Net Audit Days
Audit Manager	229	63	93	10	63
Senior Auditor *	237	64	0	10	168
Senior Auditor	261	63	0	10	188
Auditor **	190	28	0	10	152
Auditor	261	63	0	10	188
Total Net Audit Days					759
Plus Salford Internal Audit Services					45
Total Available Audit Days					804

Notes:

- The Audit Managers time has been adjusted to provide an allowance for Counter Fraud work.
- * One Senior Auditors time has been adjusted for the 20% apprentice requirement for off the job training.
- ** One Auditors time has been adjusted as they are term time only, with overheads reduced to remove the annual leave requirement.
- Overheads include annual leave, bank holidays, training, continuous improvement, and admin.
- Management includes planning, supervision, quality assurance, performance, reporting, attendance at meetings, strategies, policies and procedures, and standards assessment.
- Carry forward is an allowance for the completion of previous years' work.

6.4 As part of business continuity and the delivery of specialist audits, there are two commissioned co-sourced arrangements that support the uninterrupted delivery of the proposed audit plan. These are provided by South West Audit Partnership (SWAP) Ltd and Salford Internal Audit Services for technical IT audits.

6.5 The resources available for Counter Fraud work are:

Post	Available Days	Overheads	Net Faud Days
Audit Manager	32	n/a	32
Counter Fraud Investigator	261	64	197
Counter Fraud Investigator	261	63	198
Total Available Counter Fraud Days			427

6.6 The Assurance Service is currently undergoing a Service Review (expected to be implemented in quarter two of 2024/25) to assess existing resources and ensure they are aligned for all the services provided, and as such the resources for Internal Audit and Counter Fraud may change during 2024/25. The Audit Plan will be re-assessed when the Service Review has been completed.

7. THE AUDIT PLAN

7.1 The Audit Plan has been developed in line with the planning process detailed in section 5. The Audit Plan aims to ensure appropriate coverage of the Strategic Risks and support the delivery of the Council's priorities which are documented in **Appendix C**. This includes Internal Audit work completed in 2023/24 in relation to the Strategic Risks to demonstrate where audit work has already been completed, and where there are any gaps.

Plan Agility and Flexibility

7.2 Internal Audit has an important role in providing critical assurance and helping to advise senior management and the Audit Panel on a changing risk and controls landscape.

7.3 To comply with the PSIAS and to respond to the changing landscape, Internal Audit needs to be able to adapt and be proactive, prepared, and informed as to regulatory and Government announcements that could affect the Council's and GMPF's business.

7.4 As such, the Audit Plan is a flexible document which will be reviewed and amended throughout the year to ensure that its content reflects new and emerging risks and priorities. Therefore, whilst audit reviews are proposed, these proposals will be subject to regular review and changes applied where appropriate, with consultation with senior management and the Chair of the Audit Panel. The Audit Panel will be provided with regular updates on any significant changes to the Audit Plan, and the reasons for the changes.

7.5 Requests from Directors to defer or remove audit reviews from the Audit Plan will need to be approved by the Head of Assurance and the Director of Resources as S151 Officer.

Resource Allocation

7.6 Internal Audit place the focus on outcomes rather than time management with each auditor being allocated a portfolio of audits and given responsibility (with the support of their manager) to deliver those assignments by a target date.

7.7 The use of audit days is purely for annual planning purposes.

Proposed Programme of Work for 2024/25

7.8 The proposed programme of Work for 2024/25 (the Audit Plan) is contained at **Appendix A** and is based on the available resources as outlined in this document. As detailed above, consultation will be ongoing throughout the year, and therefore the proposed assignments are likely to change.

7.9 Detailed Terms of Reference will be agreed with auditees, including senior management, prior to each audit assignment commencing.

8. COLLABORATION

8.1 The Head of Assurance participates in the North West Chief Audit Executives Group, which meets regularly and acts as a discussion group on various local and national developments affecting Internal Audit. The group also has several sub-groups on specific areas relevant to the work of Internal Audit and Counter Fraud, for sharing best practice and learning from colleagues.

8.2 When beneficial and practical, audit work may be undertaken with other partner authorities. The benefits of participation should increase assurances available for all partners, to develop strong working relationships and to provide positive learning experiences.

9. ARRANGEMENTS FOR REPORTING INTERNAL AUDIT WORK

9.1 At the conclusion of each audit assignment, a draft report is issued to the manager responsible for the audit area. Once responses have been received and agreed, a final report is issued to:

- The Chief Executive
- The Director of Resources (S151 Officer)
- The Director and Assistant Director responsible for the audit area
- Finance Business Partner
- Executive Member
- The Council's External Auditor

9.2 Each report includes an overall assurance rating and any recommendations made are graded in terms of priorities. The Assurance Recommendations and Classifications are detailed in **Appendix B**.

9.3 Internal Audit reviews quality and improvement in line with the Quality Assurance & Improvement Programme, presented alongside this Strategy and Plan. The outcomes of activity are included in progress reports and the annual report.

APPENDIX 1

- 9.4 Throughout the year, regular progress reports are presented to the Audit Panel summarising the outcomes of work completed, and any significant matters identified.
- 9.5 An annual report is presented to the Audit Panel, which includes the Head of Assurance's overall opinion on the Council's governance, risks management and control environment. The opinion forms one source of assurance in support of the Council's Annual Governance Statement (AGS). The opinion is based on the findings from the work of Internal Audit completed during the year, and other sources of assurance received by the Council, such as external regulators.

PROPOSED PROGRAMME OF WORK FOR 2024/25 (THE AUDIT PLAN)

Tameside Internal Audit Plan

Audit Theme / Area This is based on the current risk assessment and will be subject to review and amendment due to changing priorities.	Drivers Strategic Risks and Corporate Priorities	Context The detailed scope of any areas subject to review will be determined when preparing for the individual audit assignment.
Core Financial Systems		
<ul style="list-style-type: none"> • Payroll • Accounts Payable • Income • Accounts Receivable • Council Tax • Business Rates • Benefits • Treasury Management • Capital Programme • Medium Term Financial Plan • Budgetary Control • General Ledger 	SR1	To provide an opinion on the adequacy and effectiveness of controls in place to mitigate key risks. Reviews will evaluate and test the effectiveness of the key controls within core financial systems, including the management of the risk of fraud and error, and the potential for material misstatement in the financial statements. The reviews completed will either be a detailed audit review or a short walk through of key controls, based on a risk assessment and previous Internal Audit work completed. The reviews will contribute to assurance for GMPF.
Key Risks and Priorities		
Adults: <ul style="list-style-type: none"> • Assessment Process • Quality Assurance Framework • Direct Payments • Demand Management 	SR1 SR2 SR3 SR4 CP8	Outcome from reviewing key risk areas. Outcome from reviewing key departmental and service risk areas. Arrangements for key service delivery areas, reviewing performance management and achievement of outcomes.
Childrens: <ul style="list-style-type: none"> • Demand Management • Children's Improvement Plan • Adoption and Fostering Payments • Delivering Better Value • SEND • Social Care and Residential Placements 	SR1 SR2 SR3 SR6 CP3	Outcome from reviewing key risk areas. Outcome from reviewing key departmental and service risk areas. Arrangements for key service delivery areas, reviewing performance management and achievement of outcomes.

Audit Theme / Area This is based on the current risk assessment and will be subject to review and amendment due to changing priorities.	Drivers Strategic Risks and Corporate Priorities	Context The detailed scope of any areas subject to review will be determined when preparing for the individual audit assignment.
Place: <ul style="list-style-type: none"> Homelessness Strategy Regeneration and Growth Climate Change 	SR8 SR10 SR12 CP5 CP6	Outcome from reviewing key risk areas. Provision for assurance on arrangements for key service delivery areas, reviewing performance management and the achievement of outcomes, and delivery of key projects and strategies.
Population Health: <ul style="list-style-type: none"> Health Protection Sexual Health 	SR2 SR6	Outcome from reviewing key risk areas. Outcome from reviewing key departmental and service risk areas. Arrangements for key service delivery areas, reviewing performance management and achievement of outcomes.
Governance and Cross-Cutting: <ul style="list-style-type: none"> Performance Management Transformation Financial Management Contract Management Use of Cash and Cards Grant Funding Emergency Planning 	SR1 SR4 SR9 SR11	Outcome from reviewing key risk areas for key corporate and cross-cutting services. Provision of assurance on the effectiveness of the Council's internal control and governance arrangements in respect of these arrangements.
ICT and Information Governance		
<ul style="list-style-type: none"> TBC following completion of 2023/24 Cyber Data Protection Accountability Records Management Information Requests 	SR5	To provide an opinion on the adequacy and effectiveness of controls in place to mitigate key risks. Provision of assurance on the effectiveness of the Council's internal control and governance arrangements in respect of these arrangements. Compliance with legislation.
Schools and Education		
<ul style="list-style-type: none"> Primary Schools Secondary Schools 	SR3 SR4 CP1 CP2	Completion of the school audit programme for a sample of schools taking into consideration the School's Financial Value Standards and a risk assessment of each individual school.
Other Activity		
Grant Certifications	SR1	Assurance work on grants requiring sign off by the Head of Assurance

Audit Theme / Area This is based on the current risk assessment and will be subject to review and amendment due to changing priorities.	Drivers Strategic Risks and Corporate Priorities	Context The detailed scope of any areas subject to review will be determined when preparing for the individual audit assignment.
Systems Development	n/a	Consultancy and advisory role to be undertaken where key systems development work is ongoing
Recommendation Tracking	n/a	Monthly reporting with Directorates, Schools and GMPF
Formal Follow Up Reviews	n/a	Formal follow up work of high-risk areas
Contingency	n/a	Including investigation into irregularity, advice, guidance, and consultancy

GMPF Internal Audit Plan

Audit Theme / Area This is based on the current risk assessment and will be subject to review and amendment due to changing priorities.	Drivers GMPF Risks	Context The detailed scope of any areas subject to review will be determined when preparing for the individual audit assignment.
ICT and Digital	45/46	Work to be determine following completion of the 2023/24 cyber review
Employer Audits	Various	Standard audit programme on a number of employers on a risk basis
Treasury Management	13	Assurance opinion on adequacy of arrangement following planned changes
Core Financial Systems	48-54	To be completed alongside Tameside core financial system audits
Data Protection	35	To be completed alongside Tameside data protection audits
McCloud	21	Review to provide assurance regarding implementation
Northern LGPS Collaborative Work	Various	Partnership with Merseyside and West Yorkshire Pension Funds

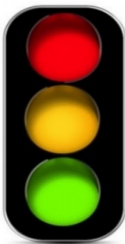
Counter Fraud Plan

Counter Fraud Theme / Area	Drivers	Context
National Fraud Initiative (NFI)	SR1	Statutory requirement responding to data matches of potentially fraudulent activity
Proactive Counter Fraud Work	SR1	Counter Fraud Policy and Strategy review Counter Fraud training, development of a mandatory e-learning module for all staff as well as bespoke briefings Based on a risk assessment, completion of proactive Counter Fraud reviews to assess fraud controls and potentially detect fraudulent activity

Counter Fraud Theme / Area	Drivers	Context
Reactive Counter Fraud Work	SR1	Risk assessment of receipt of allegations to determine action to be in line with the Counter Fraud Strategy

ASSURANCE AND RECOMMENDATION CLASSIFICATIONS

Overall Audit Assurance Opinion	Definition
Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

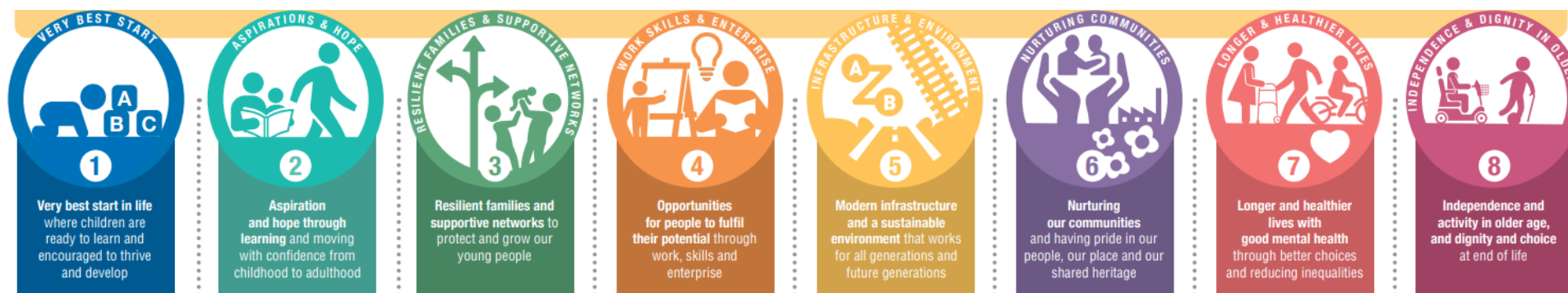
Priority	Definition
	High Priority Recommendation Representing a fundamental control weakness which exposes the organisation to a high degree of unnecessary risk.
	Medium Priority Recommendation Representing a significant control weakness which exposes the organisation to a moderate degree of unnecessary risk.
	Low Priority (housekeeping) Recommendation Highlighted opportunities to implement a good or better practice, to add value, improve efficiency or further reduce the organisation's exposure to risk.

STRATEGIC RISKS

Risk No.	Risk Title	Residual Risk Rating	2023/24 Internal Audit Work / External Regulator
SR1	Financial Resilience	20	Budgetary Control, Budget Challenge, Medium Term Financial Planning, Direct Payments
SR2	Capacity of the Workforce	16	Commissioning, Strategic Procurement, Recruitment and Retention, Agency Workers
SR3	Safeguarding Adults and Children	16	Schools, Ofsted Inspection
SR4	Poor Performance and Improvement Plans	16	Schools, Ofsted Inspection
SR5	Cyber Security	16	Cyber Security, PCI Compliance
SR6	Wider Socio Economic Environment	15	Major Programmes
SR7	Health & Social Care Reform	12	Health & Social Care Reform
SR8	Inability to Drive Growth	12	Major Programmes
SR9	Key Supplier / Partner Failure	8	Adults Contract Commissioning
SR10	Housing Supply	8	Major Programmes
SR11	Resilience	8	None
SR12	Climate Change	8	None

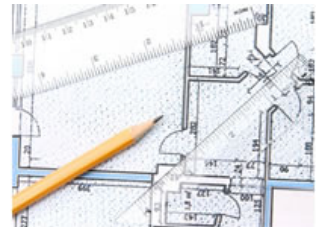
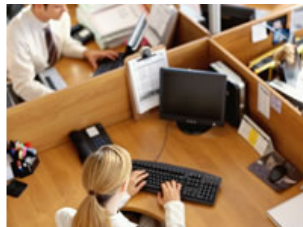
Page 123

CORPORATE PRIORITIES



This page is intentionally left blank

ASSURANCE SERVICE INTERNAL AUDIT CHARTER 2024/25



January 2024

APPENDIX 2

BACKGROUND

The purpose of this Internal Audit Charter is to define Internal Audit's purpose, authority, and responsibility. It establishes Internal Audit's position within the Council and reporting lines, authorises access to records, personnel, and physical property relevant to the performance of audit work, and defines the scope of internal audit activities.

STANDARDS

The Internal Audit function is required to comply with the Public Sector Internal Audit Standards (PSIAS). The Relevant Internal Audit Standard Setters, which includes the Chartered Institute of Public Finance and Accountancy (CIPFA) and the Chartered Institute of Internal Auditors (CIIA) in respect of local government, have adopted the common set of standards. The PSIAS encompass all of the mandatory elements of the Chartered Institute of Internal Auditors International Professional Practices Framework (IPPF). Compliance with the Standards is subject to an ongoing quality assurance and improvement programme (QAIP) developed by Internal Audit to ensure continuous compliance with the Standards.

The mission and definition for Internal Audit are defined by the PSIAS and detailed below:

MISSION

'To enhance and protect organisational value by providing risk-based and objective assurance, advice, and insight.'

DEFINITION

'Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.'

In undertaking this role Internal Audit satisfies the statutory duties of the Council's Section 151 Officer (Local Government Act 1972) and the Accounts and Audit Regulations 2015.

The Head of Assurance fulfils the Chief Audit Executive role as defined by the PSIAS.

The PSIAS also require Internal Audit to define the following terms in respect of the Audit function:

The Board

For the purposes of internal audit, the 'Board' refers to the Councils' Audit Panel/ Greater Manchester Pension Fund (GMPF) Local Board. The Board provides an independent review of the audit, assurance and reporting arrangements that underpin good governance and financial standards.

Senior Management

Senior management is defined as the Chief Executive and members of the Council's Senior Leadership Team (SLT).

Statutory Officers

The Council's statutory officers include:

- Head of Paid Service – Chief Executive
- Section 151 Officer – Director of Resources
- Monitoring Officer – Assistant Director Legal/Borough Solicitor

APPENDIX 2

RESPONSIBILITY AND OBJECTIVES OF INTERNAL AUDIT

Internal Audit is responsible for establishing procedures and applying the required resources to ensure that the service conforms with the Definition of Internal Auditing and the Standards. The members of the Internal Audit Team must demonstrate conformance with the Code of Ethics and the Standards.

The Head of Assurance must deliver an Annual Audit Opinion and report that can be used by the organisation to inform its Annual Governance Statement (AGS). The Annual Audit Opinion must conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control. This is the 'assurance role' for Internal Audit.

Internal Audit may also provide an independent and objective consultancy service, which is advisory in nature and generally performed at the specific request of the organisation. The aim of the consultancy service is to help management improve the Council's governance, risk management, and internal control. This is the 'Consultancy' role for Internal Audit and contributes towards the overall opinion.

RESPONSIBILITIES OF THE COUNCIL

The Council is responsible for ensuring that Internal Audit is provided with all necessary assistance and support to ensure that it meets the required standards.

The Section 151 Officer will make appropriate arrangements for the provision of an Internal Audit Service. This will include the formal adoption of this Charter by the Audit Panel and the adoption of corresponding elements in the Financial Regulations.

The Council will ensure it has taken all necessary steps to provide Internal Audit with information on its objectives, risks, and controls to allow the proper execution of the Audit Strategy and adherence to internal audit standards. This will include notifying Internal Audit of any significant changes in key control systems which may affect the Audit Plan.

The Council, through the Chief Executive, Section 151 Officer, and other relevant managers, will respond promptly to audit plans, reports, and recommendations.

Responsibility for monitoring and ensuring the implementation of agreed recommendations rests with the managers within the Council.

INDEPENDENCE OF INTERNAL AUDIT

Internal Audit operates independently of all the activities within the Council to ensure that it is able to appraise the Authority's governance, risk management and internal control systems in an impartial and unbiased manner. It is the responsibility of executive directors, directors and service managers to maintain effective systems of governance and control.

To ensure this independence, Internal Audit operates within a framework that allows access to all Council Officers, Senior Managers and elected Members. As such, all Internal Audit staff have the right to all documentation held by the Council and to seek explanations from all officers and Elected Members of the Council, as they see necessary to effectively discharge their duties.

In addition to managing Internal Audit, the Head of Assurance has line management responsibility for Risk, Insurance, and Information Governance. Arrangements have been established to mitigate any potential impairment to independence and objectivity in relation to the audit of these areas. These arrangements will involve the Audit Manager reporting the findings from these audits directly to the Director of Resources, without any influence by the Head of Assurance, or opt to utilise independent, external assurance providers for this work.

APPENDIX 2

All auditors are required to complete and sign a Code of Ethics and Declaration of Interest Statement on an annual basis. Where auditors have a perceived conflict of interest in undertaking a piece of work, this will be managed through the internal audit management and supervision process.

The Head of Assurance will implement safeguards to ensure that individual auditors remain independent of areas they are auditing by ensuring staff are not involved in auditing areas where they have had recent operational involvement or where they have provided consultancy and advice. Auditors will be rotated so that they do not perform the same audit more than three years continuously.

HEAD OF ASSURANCE

The Head of Assurance will be appointed in accordance with the Council's Recruitment and Selection Policy and will have sufficient skills, experience, and competencies to work with the Single Leadership Team, the Audit Panel, and the GMPF Local Board to influence the governance, risk management, and internal control of the Council.

The Head of Assurance is responsible for ensuring that there is access to the full range of knowledge, skills, qualifications, and experience to deliver the Audit Plan and meet the requirements of the PSIAS. In addition to internal audit skills, the Head of Assurance will specify any other professional skills that may be needed by the Internal Audit Team. The Head of Assurance will hold a full, professional qualification, defined as CCAB, CMIIA or equivalent professional membership and adhere to professional values and the Code of Ethics.

RELATIONSHIPS

The Head of Assurance reports directly to the Director of Resources (Section 151 Officer). The Head of Assurance, or an appropriate representative of the Internal Audit Team, shall attend meetings of the Audit Panel and the GMPF Local Board unless, exceptionally, the Panel/Board decides that they should be excluded from either the whole meeting or for particular agenda items.

The Head of Assurance shall have an independent right of access to the Chair of the Audit Panel and GMPF Local Board. In exceptional circumstances, where normal reporting channels may be seen to impinge on the objectivity of the audit, the Head of Assurance may report directly to the Chair of the Audit Panel or GMPF Local Board.

Internal Audit and External Audit will agree a protocol for co-operation which will make optimum use of the available audit resources.

SCOPE OF INTERNAL AUDIT

The Head of Assurance will develop and maintain a strategy for providing the Chief Executive and the Section 151 Officer economically and efficiently, with objective evaluation of, and opinions on, the effectiveness of the Council's governance, risk management, and internal control arrangements. The Audit Plan will be risk based, prepared in consultation with senior management and Executive Members and be presented to the Audit Panel and GMPF Local Board for approval. The Head of Assurance Annual Opinion is a key element in the framework of assurance that the Chief Executive and the Executive Leader of the Council need to inform the completion of the AGS.

OPINION WORK

The Internal Audit activity must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach that is aligned with all of the strategies, objectives and risks to the Council.

GOVERNANCE

Internal Audit must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- promoting appropriate ethics and values within the organisation;
- ensuring effective organisational performance management and accountability;
- communicating risk and control information to appropriate areas of the organisation; and
- co-ordinating the activities of and communicating information among the Audit Panel and GMPF Local Board, External and Internal Auditors and management.

RISK MANAGEMENT

Internal Audit must evaluate the effectiveness and contribute to the improvement of risk management processes by assessing that:

- organisational objectives support and align with the organisation's vision;
- significant risks are identified and assessed;
- appropriate risk responses are selected that align risks with the organisation's risk appetite; and
- relevant risk information is captured and communicated in a timely manner across the organisation, enabling staff, management, and the board to carry out their responsibilities.

INTERNAL CONTROL

Internal Audit must assist the organisation in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. The Internal Audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organisation's governance, operations, and information systems regarding the:

- achievement of the organisation's strategic objectives;
- reliability and integrity of financial and operational information;
- economical, effective and efficient use of resources;
- effectiveness and efficiency of operations and programmes;
- safeguarding the Council's assets and interests from losses of all kinds, including those arising from fraud, irregularity corruption or bribery; and
- compliance with laws, regulations, policies, procedures, and contracts.

Internal Audit proactively identify audits to address any emerging and developing risks on an ongoing and 'future focussed' basis.

Internal Audit will promote and contribute to continuous ongoing improvements in systems across the Council by identifying and recommending best practice actions following audit work completed.

Where key systems are being operated on behalf of the Council or where key partnerships are in place the Head of Assurance must ensure arrangements are in place to form an opinion on their effectiveness.

Where the Council operates systems on behalf of other bodies, the Head of Assurance must be consulted on the audit arrangements proposed or in place.

It is management's responsibility to ensure the provision for relevant audit rights of access in any contract or Service Level Agreement the Council enters into, either as provider or commissioner of the service.

APPENDIX 2

NON – OPINION WORK

Internal Audit may provide, at the request of management, a consultancy service which evaluates the policies, procedures and operations put in place by management. A specific contingency should be made in the Internal Audit Plan to allow for management requests and consultancy work.

The Head of Assurance must consider the effect on the opinion work before accepting consultancy work or management requests over and above the contingency allowed for in the Audit Plan. In the event that the proposed work may jeopardise the delivery of the Audit Opinion, the Head of Assurance must advise the Section 151 Officer before commencing the work. The Head of Assurance must consider how the consultancy work contributes towards the overall opinion.

FRAUD

Managing the risk of fraud is the responsibility of line management; however, the Section 151 Officer retains specific responsibilities in relation to the detection and investigation of fraud. The Internal Audit Service provides a Counter Fraud function that includes undertaking work of a proactive nature, conducting substantive audits in key risk areas as well undertaking some reactive work of an investigatory nature involving suspected fraud.

In addition, the service is responsible for maintaining effective counter fraud policies and procedures for the Council.

Internal Audit should be notified of all suspected or detected fraud, corruption, or impropriety, to inform their opinion on the control environment and the Audit Plan.

REPORTING

The Head of Assurance will agree reporting arrangements with the Chief Executive and the Section 151 Officer which will include procedures for the:

- distribution and timing of draft audit reports;
- Council's responsibilities in respect of responding to draft audit reports;
- distribution of finalised audit reports;
- follow up by Internal Audit of agreed recommendations; and
- escalation of recommendations where management responses are judged inadequate in relation to the identified risks.

The Head of Assurance will present a formal report annually to the Chief Executive, Section 151 Officer, the Audit Panel and GMPF Local Board giving an opinion on the overall adequacy and effectiveness of the Council's framework of governance, risk management, and internal control. This report will conform to the PSIAS for the Head of Assurance and will be timed to support the production of the Council's AGS.

Reports of progress against the planned work will be presented to the Audit Panel and GMPF Local Board on a regular basis during the year.

INTERNAL AUDIT ACCESS RIGHTS

Designated auditors are entitled, without necessarily giving prior notice, to require and receive from the Council and any associated or contracted bodies including any shared service providers or trading companies:

- access to all records, documents and correspondence relating to any financial or other relevant transactions, including documents of a confidential nature;

APPENDIX 2

- access at all reasonable times to any land, premises, officer and member of the Council;
- the production of any cash, stores, or other property of the Council under an officer's and member's control; and
- explanations concerning any matter under investigation.

INTERNAL AUDIT RESOURCES

If the Head of Assurance or the Audit Panel and GMPF Local Board consider that the level of audit resources or the terms of reference in any way limit the scope of Internal Audit, or prejudice the ability of Internal Audit to deliver a service consistent with the Definition of Internal Auditing and the Standards, they should advise the Chief Executive and the Section 151 Officer accordingly.

QUALITY ASSURANCE & IMPROVEMENT PROGRAMME

The PSIAS require a Quality Assurance & Improvement Programme (QAIP) to be developed and maintained that covers all aspects of Internal Audit activity.

The QAIP is designed to provide reasonable assurance to key stakeholders that Internal Audit:

- Performs its work in accordance with the Charter.
- Operates in an effective and efficient manner.
- Is adding value and continually improving the service that it provides.

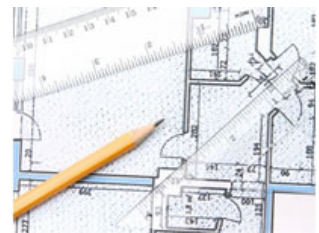
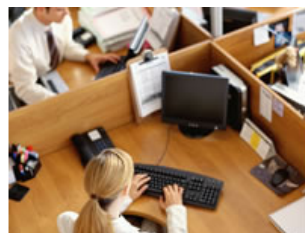
The QAIP conforms to the requirements of the PSIAS and provides for both internal and external assessments. Internal assessments are both ongoing and periodical, and external assessments must be undertaken at least once every five years.

REVIEW

This Charter will be reviewed periodically by the Head of Assurance and presented to the Audit Panel for approval

This page is intentionally left blank

ASSURANCE SERVICE INTERNAL AUDIT QUALITY ASSURANCE & IMPROVEMENT PROGRAMME 2024/25



January 2024

APPENDIX 3

1. Introduction

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

2. Internal Assessments

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

On-going Reviews

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

Periodic Reviews

- 2.3 Periodic assessments are designed to assess conformance with Internal Audit's Strategy, Charter, the PSIAS Mission and Definition of Internal Auditing, the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, and the efficiency and effectiveness of Internal Audit in meeting the needs of its various stakeholders. Periodic assessments are conducted through:

- Regular Update Reports, presented to the Audit Panel and the GMPF Local Board;
- Annual risk assessments, in accordance with the Audit Charter 2023/24 and the Audit Manual, for the preparation of the Audit Plan;
- Annual review of the Effectiveness of Internal Audit, undertaken by the Head of Assurance, using the PSIAS standards as the basis for the self- assessment;
- Annual review of compliance against the requirements of this QAIP, the results of which are reported to the Audit Panel;
- Feedback from the Director of Resources and Audit Panel to inform the annual appraisal of the Head of Assurance, in accordance with Standard 1100;
- My Performance reviews conducted for each auditor based on the principles of the CIPFA Guidance document “The Excellent Internal Auditor” (2010) to inform the appraisal process and identify individual training and development needs.

Performance Indicators

- 2.4 Performance indicators are in place to monitor the audit team productivity and customer feedback:
- Audit Assignment (target 90%) – this will be measured as the number of audit assignments completed by the target date.
 - Customer Satisfaction (target 90%) – this will be measured through the completion of post audit questionnaires.
 - Value Added (target 90%) – this will be measured through the number of audit clients who expressed that the audit added value from the post audit questionnaire.
- 2.5 In addition, performance indicators are in place to monitor the Council’s performance in terms of implementation of recommendations, on a Directorate basis:
- High Recommendations (90% target) – this will be measured by the number of high priority recommendations implemented by the agreed implementation date.
 - Medium Recommendations (90% target) – this will be measured by the number of medium priority recommendations implemented by the agreed implementation date.

3. EXTERNAL ASSESSMENTS

- 3.1 External assessments will appraise and express an opinion about Internal Audit’s conformance with the PSIAS Mission of Internal Audit, Definition of Internal Auditing and Code of Ethics and include recommendations for improvement, as appropriate.

Frequency of External Assessment

- 3.2 An external assessment will be conducted at least every five years, in accordance with the PSIAS. A system of Peer Reviews will be undertaken across the North West Chief Audit Executive Group. The Council’s Internal Audit Service was assessed in March 2018 and was judged to conform to the standards, some minor recommendations were made during the Peer Review and these are detailed in Section 4 below. The next external assessment is due to be completed in quarter four 2023/24.
- 3.3 With the introduction of the new standards due to be effective from 2025, consideration will be given to procuring an external assessment from CIPFA.

Scope of External Assessment

- 3.4 The external assessment will consist of a broad scope of coverage that includes the following elements of Internal Audit activity:
- Conformance with the *Standards*, Mission of Internal Audit, Definition of Internal Auditing, the Code of Ethics, and Internal Audit’s Charter, Strategy, plans, policies, procedures, practices, and any applicable legislative and regulatory requirements;

- Integration of the Internal Audit activity into Tameside's governance framework, including the audit relationship between and among the key groups involved in the process;
- Tools and techniques used by Internal Audit;
- The mix of knowledge, experiences, and disciplines within the staff, including staff focus on process improvement delivered through this QAIP;
- A determination whether Internal Audit adds value and improves Tameside's operations.



4. REPORTING

- 4.1 The outcome of internal assessments and any external assessments will be reported to the Director of Resources and the Audit Panel/GMPF Local Board. The Head of Assurance will not state that the Internal Audit Service conforms with the PSIAS unless the results of the QAIP (including a completed external assessment) confirm this.
- 4.2 The Head of Assurance will implement appropriate follow-up to any identified actions to ensure continual improvement of the service.
- 4.3 Progress in implementing agreed improvement plans will be included as part of the Annual Report to the Audit Panel/GMPF Local Board.
- 4.4 Any significant areas of non-compliance with the PSIAS will be reported in the Head of Assurance's Annual Report, which is used to inform the Annual Governance Statement (AGS).

5. REVIEW OF THE QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME

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

Agenda Item 9.

Report to:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Carol McDonnell – Head of Assurance
Subject:	AUDIT PANEL WORK PROGRAMME 2023/24
Report Summary:	This report details the updated Audit Panel Work Programme for 2023/24.
Recommendations:	That the Audit Panel Work Programme for 2023/24 at Appendix 1 is noted.
Corporate Plan:	Having a comprehensive Audit Panel work programme in place, provides assurance to the Council that the Panel is fulfilling its terms of reference in accordance with best practice. Through regular risk updates, the Panel seeks assurance that risks associated with the delivery of the Corporate Plan are being managed.
Policy Implications:	As above.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	There are no financial implications directly associated with this report.
Legal Implications: (Authorised by the Borough Solicitor)	A dedicated, effective Audit Panel with a comprehensive work programme is key to supporting good governance, strong financial management and effective internal and external audit and is in accordance with the latest CIPFA guidance 'Audit Committees: Practical Guidance for Local Authorities and Police 2022'.
Risk Management:	As above.
Background Information:	The background papers can be obtained from the author of the report, Carol McDonnell, Head of Assurance:  0161 342 3231  carol.mcdonnell@tameside.gov.uk

This page is intentionally left blank


AUDIT PANEL WORK PLAN 2023/24

Item	Lead	Aug 2023	Sep-2023	Nov 2023	Jan 2024	March 2024	Comments
Finance							
Annual Treasury Report / Prudential Indicators	S151	✓					
Treasury Update	S151			✓	✓		
Draft Statement of Accounts	S151	✓					2022/23
Audited Statement of Accounts for Approval	S151	✓			✓	✓	2020/21 (Aug 23), 2021/22 (Jan 24), 2022/23 (Mar 24)
Annual Report of Exceptions to Contract Procedure Rules	S151/MO				✓		
CIPFA Financial Management Code / Local Audit Update	S151				✓		Only relevant if updates to guidance
Internal Audit							
Chair of the Committee's Annual Report	HoA	✓					
Internal Audit Annual Report	HoA	✓					
Internal Audit Plan, Charter & Protocol	HoA	✓*				✓	*Refreshed Plan
Internal Audit Progress Report	HoA			✓	✓		
Public Sector Internal Audit Standards external review	HoA						To be presented in June 2024
Quality Assurance & Improvement Programme	HoA					✓	With the Audit Plan
Counter Fraud Update Report Including Counter Fraud & Corruption / Whistleblowing / Anti Money Laundering / Prevention of Tax Evasion Policies	HoA				✓		
Governance & Performance							
Annual Governance Statement	S151/HoA	✓					
Annual Governance Statement – Actions Follow Up	S151/HoA			✓		✓	
Code of Corporate Governance Review	S151/HoA	*					*To be presented with the AGS
Information Governance Policies e.g., Data Protection, GDPR	HoA					✓	

Item	Lead	Aug 2023	Sep 2023	Nov 2023	Jan 2024	March 2024	Comments
Annual Investigatory Powers Act Report	MO						To be presented in 24/25
CIPFA Audit Committee Guidance and Effectiveness	HoA			✓			
Assurance Reports from Other Assurance Providers e.g., OFSTED, CQC etc.							As and when received
Risk Management							
Risk Management Policy / Review	HoA			✓*			*Included in risk update
Quarterly Risk Management Updates	HoA	✓		✓	✓		
External Audit							
Tameside Council Audit Completion Report	EA	✓			✓	✓	
Greater Manchester Pension Fund Audit Completion Report	EA	✓		✓	✓	✓	
Tameside Council Audit Strategy Memorandum	EA	✓			✓		
Progress Report	EA					✓	
Private Meeting with the Internal and External Auditors	EA/HoA	✓	✓	✓	✓	✓	
External Audit Appointment	S151	✓					
Audit Panel Work Programme / Training							
Audit Panel Work Programme		✓	✓	✓	✓	✓	At every meeting
Audit Committee Training – Webinar (Diana Melville, CIPFA)	CIPFA						Held on 8 August 2023 via webinar.

S151 = Director of Resources / S151, HoA = Head of Assurance, EA = External Auditor (Mazars), MO = Deputy Monitoring officer

Report to:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Ilys Cookson – Assistant Director, Exchequer Services
Subject:	STATEMENT OF LOCAL AUTHORITY CLAIMED ENTITLEMENT TO HOUSING BENEFIT SUBSIDY FOR FINANCIAL YEAR 2022/2023
Report Summary:	<p>The Council administers Housing Benefit for the Department of Work and Pensions in accordance with legislation.</p> <p>The Council is reimbursed, in part, for the cost of the Housing Benefit payments made in each financial year. To claim the costs the Council must submit an audited subsidy statement.</p>
Recommendations:	That the Audit Panel note the audited final subsidy claim for the financial year 1 April 2022 to 31 March 2023.
Corporate Plan:	The report supports the “Nurturing our Communities” and “Live Longer and Healthier Lives” Corporate Plan priority themes.
Policy Implications:	The audit and reporting of subsidy claimed accords with good financial practice.
Financial Implications: (Authorised by the statutory Section 151 Officer & Chief Finance Officer)	<p>The Council is required to submit an initial estimate, a mid-year estimate and a final housing benefit subsidy claim to the Department for Work and Pensions known as the “statement of local authority claimed entitlement to housing benefit for the financial year”.</p> <p>The final claim is then subject to an independent audit. This report provides details of the audit outcome and resulting adjustment of the 2022/23 subsidy claim made by the Council that was in excess of £55m of housing benefit payments. The outcome was a favourable adjustment of £0.009m for the Council.</p> <p>The audit concludes the claim process for the 2022/23 financial year and there are no additional implications on the Council budget.</p>
Legal Implications: (Authorised by the Borough Solicitor)	<p>The report is for noting and provides assurance with regard to the quality of the Council’s auditing and recording of subsidy claimed in relation to Housing Benefits payments made by the Department for Work and Pensions to the Council in accordance with the Income-related Benefits (Subsidy to Authorities) Order 1998.</p> <p>The report indicates that there are no concerns in relation to the final subsidy claim following an external audit process.</p>
Risk Management:	Risk Assurance is set out in section 3 of this report.
Background Information:	The background papers relating to this report can be inspected by contacting Ilys Cookson, Assistant Director, Exchequer Services.

 Telephone: 0161 342 4056

 e-mail: ilyc.cookson@tameside.gov.uk

1. INTRODUCTION

- 1.1 Local authorities administer Housing Benefit on behalf of the Department of Work and Pensions (DWP).
- 1.2 The Council is reimbursed by the DWP for the expenditure for Housing Benefit. The funding provided to pay Housing Benefit is called subsidy. The DWP pay subsidy to local authorities in accordance with the Income-related Benefits (Subsidy to Authorities) Order 1998.
- 1.3 At the beginning of each financial year, the Council submit the estimated cost of Housing Benefit to the DWP. Based on this information the DWP make a monthly payment to the Council.
- 1.4 At the end of each financial year, a final claim is made to the DWP for the actual amount of Housing Benefit expenditure made during that year. The claim is called the "Statement of local authority claimed entitlement to Housing Benefit subsidy for the financial year". The Statement for 2022/2023 is at **Appendix 1**.
- 1.5 The Housing Benefit claim is then audited by external auditors. The auditors for 2022/2023 were KPMG.

2. THE AUDIT PROCESS

- 2.1 KPMG completed the audit for 2022/2023 and reported their findings on 13 December 2023.
- 2.2 KPMG found amendments to the Subsidy claim as follows:
 - An under claim of subsidy in relation to the War Widows Pension Modified Scheme.
 - An overclaim of subsidy in relation to the classification of overpaid Housing Benefit.The resulting change in subsidy for 2022/2023 in respect of a claim in excess of £55m was an adjustment of £8,577.
- 2.3 This is a very good outcome for the Council, which has no financial implications for the Council's budget.
- 2.4 To audit the claim, KPMG undertake the DWP's Housing Benefit (Subsidy) Assurance Process (HBAP). The DWP provide modules within the HBAP that the auditors are required to test. Specifically, the auditors are required to test the following:
 - Module 2 – Uprating – checking that the parameters within the Council's system are using the correct benefit amounts to calculate benefit entitlement and claim subsidy correctly.
 - Module 3 – Workbooks – the Council prepare detailed testing workbooks of randomly selected claims for the auditors to check that subsidy has been calculated and claimed correctly. Information as to how subsidy is claimed and calculated can be found at **Appendix 2**.
 - Module 5 – Software diagnostic tool – the software used to calculate the subsidy to be claimed is tested to confirm that the benefit granted has been reconciled with the benefit paid.
 - Module 6 – Testing Strategy and reporting requirements – the mechanism for testing, error types and the recording and amending of errors reported and on the Final Claim.Module 1 is the framework for the auditors on how to conduct the audit and Module 4 is an internal document for the DWP, which is not published.
- 2.5 Where the auditors find errors in the claims identified in the testing workbooks, further testing of an extended sample of claims will take place to arrive at a more representative calculation. This is called the extrapolation calculation. The calculation means that the value of the errors identified in a particular cell can be increased to represent if the same errors had been made

in relation to the full amount claimed in that cell. This can have a significant financial implication for the Council if the subsidy claim is reduced leaving a shortfall from the amount of benefit paid which is funded from the Council's budget.

- 2.6 Where a Council has been found to have made a number of errors, the subsequent years workbooks will require additional volumes of claims to be checked. This is called Cumulative Assurance Knowledge and Experience (CAKE) testing. This can be very time consuming for both the Council and the auditors.

3. RISKS AND MITIGATION

- 3.1 Officers assessing claims for Housing Benefit are provided with extensive training and provided with a manual to refer to when required. Quality checks of each member of staff's work are undertaken regularly with feedback on levels of accuracy provided in My Performance conversations.
- 3.2 The value of any overpayments, which are due to official error or delayed processing, are monitored on a weekly basis as a large increase in the amount of these overpayments have a detrimental impact for the Council. 5 Quality monitoring of work is undertaken to reduce errors.
- 3.3 Recovery of Housing Benefit overpayments is prioritised and monitored as the Council benefit where an overpayment is recovered in full and the 40% subsidy on the payment is also received.

4. CONCLUSION

- 4.1 The result of the audit of the Statement of local authority claimed entitlement to Housing Benefit subsidy for financial year 2022/2023 is positive for the Council and has no financial implications for the Council's budget.

5. RECOMMENDATIONS

- 5.1 As set out at the front of the report.

This page is intentionally left blank

**Statement of local authority claimed entitlement to
Housing Benefit subsidy for financial year ending (FYE) March 2023**

Authority Name	TAMESIDE								001
Authority Reference Number	0	0	0	2	1	1	7	5	002

Important:

1. Please read the guidance notes before you fill in this form.
2. Incorrectly completed forms may have to be returned and errors may result in payment being delayed.
3. Deadline for receipt is **30 April 2023**; deadline for receipt of the reporting accountant-assured claim is **30 November 2023**.

Final subsidy claim for Housing Benefit - FYE March 2023

Subsidy claimed for rent rebates (Cell 036S + Cell 076S)	2,136,815	003
Subsidy claimed for rent allowance (Cell 129S)	52,128,204	004
Administration subsidy received	829,671	005
Total reduction for prior year uncashed payments (Cell 179S)	0	006
Total subsidy claimed Cells (003 + 004 + 005) - (006)	55,094,690	007
Less interim benefit subsidy	57,218,163	008
Balance now owed to or by (-) authority (Cell 007 - Cell 008)	-2,123,473	009

Please provide a local authority contact:

Name: Amanda Chadderton

Telephone No. (+STD) 0161 342 2605 Ext

Completed final claim should be returned by e-mail to: HBSubsidy@dwp.gov.uk		FOR DEPARTMENT USE ONLY	
Department for Work and Pensions Local Authority Funding Team Local Authority Partnership Engagement & Delivery Housing Benefit Unit (Room B120D) Warbreck House BLACKPOOL FY2 0UZ	Telephone:	Input by	<input type="text"/>
	01253 337972	Date	<input type="text"/>
	01253 337763	Authorised	<input type="text"/>
	01253 337975	Date	<input type="text"/>
01253 337979			

Cell 010 - Spare

Rent rebates (tenants of non-Housing Rent Allowance properties)

**Total expenditure
(Benefit Granted)**

3,270,527 011

Expenditure

Rate

Subsidy

Temporary board and lodging and non-self-contained licensed accommodation where the local authority is the landlord

Expenditure **up to** the current limit
Details of limits are available in the
subsidy guidance manual.

376,450 012

1.00

376,450 012S

Expenditure **above** the current limit
Details of limits are available in the
subsidy guidance manual.

1,133,252 013

NIL

0 013S

Temporary or short term leased and self-contained licensed accommodation where the local authority is the landlord

Expenditure **up to** the current limit
Details of limits are available in the
subsidy guidance manual.

0 014

1.00

0 014S

Expenditure **above** the current limit
Details of limits are available in the
subsidy guidance manual.

0 015

NIL

0 015S

Cells 016 to 020 - Spare

Cell 021 - Scotland only

Extended payments

Total extended payments of non-HRA rent
rebates.

0 022

1.00

0 022S

Non-Housing Rent Allowance (HRA) rent rebate expenditure attracting full-rate subsidy which is included in cell 011 but not otherwise separately identified in this section

1,758,721 023

1.00

1,758,721 023S

Overpaid (non-HRA) rent rebates (current year)

DWP error overpayments recovered.

0 024

NIL

0 024S

DWP error overpayments not recovered.

260 025

1.00

260 025S

LA error and administrative delay overpayments.	1,260	026	NIL	0	026S
-------------------------------------------------	-------	-----	-----	---	------

Technical overpayments.	274	027	NIL	0	027S
-------------------------	-----	-----	-----	---	------

Eligible overpayments.	310	028	0.40	124	028S
------------------------	-----	-----	------	-----	------

Overpaid (non-HRA) rent rebates (prior years)

DWP error overpayments recovered.	0	029	NIL	0	029S
-----------------------------------	---	-----	-----	---	------

DWP error overpayments not recovered.	0	030	1.00	0	030S
---------------------------------------	---	-----	------	---	------

LA error and administrative delay overpayments.	-537	031	NIL	0	031S
-------------------------------------------------	------	-----	-----	---	------

Technical overpayments.	0	032	NIL	0	032S
-------------------------	---	-----	-----	---	------

Eligible overpayments.	0	033	0.40	0	033S
------------------------	---	-----	------	---	------

Total subsidy claimed at full rate

Cell 034S = (012S + 014S + 022S + 023S + 025S) - (029 + 031 + 032 + 033).	2,135,968	034S
------------------------------------------------------------------------------	-----------	------

Total subsidy claimed at reduced rates

Cell 035S = 028S + 033S.	124	035S
--------------------------	-----	------

Total non-HRA rent rebate subsidy claimed

Cell 036S = 034S + 035S + 208S. (The amount in cell 036S is added to the amount in cell 076S and entered in cell 003.)	2,136,815	036S
---------------------------------------------------------------------------------------------------------------------------	-----------	------

In-year reconciliation

Cell 037 = total of cells (012 to 015) and (022 to 028); this must equal the figure in cell 011.	3,270,527	037
--------------------------------------------------------------------------------------------------	-----------	-----

Backdated expenditure

0	038
---	-----

Cells 039 to 054 - Spare

Rent rebates (tenants of HRA properties)

Total expenditure (Benefit Granted)

0	055
---	-----

	Expenditure	Rate	Subsidy
Cells 056 to 057 - Wales only Cell 058 - Spare			
Extended payments			
Total extended payments of HRA rent rebates.	0 059	1.00	0 059S
Expenditure on Affordable Rents			
Total expenditure on affordable rents for properties in the HRA.	0 060	1.00	0 060S
HRA rent rebate expenditure attracting full-rate subsidy which is included in cell 055 but not otherwise separately identified in this section			
Cell 062 - Wales only	0 061	1.00	0 061S
Overpaid (HRA) rent rebates (current year)			
DWP error overpayments recovered.	0 063	NIL	0 063S
DWP error overpayments not recovered.	0 064	1.00	0 064S
LA error and administrative delay overpayments.	0 065	NIL	0 065S
Technical overpayments.	0 066	NIL	0 066S
Eligible overpayments.	0 067	0.40	0 067S
Overpaid (HRA) rent rebates (prior years)			
DWP error overpayments recovered.	0 068	NIL	0 068S
DWP error overpayments not recovered.	0 069	1.00	0 069S
LA error and administrative delay overpayments.	0 070	NIL	0 070S
Technical overpayments.	0 071	NIL	0 071S
Eligible overpayments.	0 072	0.40	0 072S
Total subsidy claimed at full rate			
Cell 073S = (059S + 060S + 061S + 064S) - (068 + 070 + 071 + 072).			0 073S
Total subsidy claimed at reduced rates			
Cell 074S = 067S + 072S.			0 074S
Cells 075 - Spare			

Total HRA rent rebate subsidy claimed

Cell 076S = 073S + 074S + 209S.

(The amount in cell 076S is added to the amount in cell 036S and entered in cell 003.)

0	076S
---	------

In-year reconciliation

Cell 077 = total of cells (059 to 061) and (063 to 067); this must equal the figure in cell 055.

0	077
---	-----

Backdated expenditure

0	078
---	-----

Cells 079 to 093 - Spare**Rent allowances****Total expenditure
(benefit granted)**

52,784,460	094
------------	-----

Expenditure

Rate

Subsidy

Regulated tenancies

Total expenditure in respect of "regulated tenancies" entered into before de-regulation.

133,251	095
---------	-----

1.00

133,251	095S
---------	------

Expenditure under the rent officer arrangements:**Cases referred to the rent officer by 30 April 2023 as required (excluding expenditure made under payments on account under reg.93 of si 2006 no.213 or reg.74 of si 2006 no.214)****Claims administered under the pre-1996 rules**

Total expenditure on that part of weekly eligible rent above the rent officer's determination on a claim where restrictions could not be made under Regs.13 or 13ZA.

367,695	096
---------	-----

0.60

220,617	096S
---------	------

Total expenditure on that part of weekly eligible rent above the rent officer's determination on a claim where restrictions could be made under Regs.13 or 13ZA. Exclude amounts in cell 096.

115,763	097
---------	-----

NIL

0	097S
---	------

Total expenditure on that part of weekly eligible rent at or below the rent officer's determination on a claim.

543,014	098
---------	-----

1.00

543,014	098S
---------	------

Maximum rent cases

Total expenditure up to the maximum rent.

877,082	099
---------	-----

1.00

877,082	099S
---------	------

**Expenditure under the rent officer arrangements:
payments made on account under reg.93 of si 2006 no. 213 or reg.74 of
si 2006 no. 214 and referral made to the rent officer by 30 April 2023**

Total expenditure arising from payments made on account under Reg.93 of SI 2006 No. 213 or Reg.74 of SI 2006 No. 214 in which a referral was made by 30 April 2023.

0	100	1.00	0	100S
---	-----	------	---	------

**Expenditure under the rent officer arrangements:
Cases requiring referral but no referral made by 30 April 2023**

Expenditure where there is no current determination and no referral made by 30 April 2023.

0	101	NIL	0	101S
---	-----	-----	---	------

**Expenditure under the rent officer arrangements:
Cases excluded from requirement to refer to the rent officer**

Total expenditure related to cases not requiring referral to the rent officer.

41,804,144	102	1.00	41,804,144	102S
------------	-----	------	------------	------

LHA expenditure

Total expenditure in claims administered under LHA rules.

8,428,092	103	1.00	8,428,092	103S
-----------	-----	------	-----------	------

Expenditure on board and lodging and non self-contained licensed accommodation provided as temporary or short term accommodation where a registered housing association is the landlord

Expenditure **up to** the current limit details of limits are available in the subsidy guidance manual.

0	104	1.00	0	104S
---	-----	------	---	------

Expenditure **above** the current limit details of limits are available in the subsidy guidance manual.

0	105	NIL	0	105S
---	-----	-----	---	------

Expenditure on self-contained licensed accommodation and accommodation owned or leased by a registered housing association provided as temporary or short term accommodation where a registered housing association is the landlord

Expenditure **up to** the current limit details of limits are available in the subsidy guidance manual.

0	106	1.00	0	106S
---	-----	------	---	------

Expenditure **above** the current limit details of limits are available in the subsidy guidance manual.

0	107	NIL	0	107S
---	-----	-----	---	------

Cell 108 Spare

Extended payments

Total extended payments of rent allowance.

3,840	109	1.00	3,840	109S
-------	-----	------	-------	------

Rent allowance expenditure attracting full-rate subsidy which is included in cell 094 but not otherwise separately identified in this section

0	110	1.00	0	110S
---	-----	------	---	------

Overpaid rent allowances (current year)

DWP error overpayments recovered.

0	111	NIL	0	111S
---	-----	-----	---	------

DWP overpayments not recovered.

3,059	112	1.00	3,059	112S
-------	-----	------	-------	------

LA error and administrative delay overpayments.

124,743	113	NIL	0	113S
---------	-----	-----	---	------

Eligible overpayments.

383,777	114	0.40	153,511	114S
---------	-----	------	---------	------

Duplicate payments.

0	115	0.25	0	115S
---	-----	------	---	------

Recovered overpayments resulting from the use of payments on account made under Reg.93 of SI 2006 No. 213 or Reg.74 of SI 2006 No.214.

0	116	NIL	0	116S
---	-----	-----	---	------

Overpayments resulting from the use of payments on account made under Reg.93 of SI 2006 No. 213 or Reg.74 of SI 2006 No.214 which have not been recovered.

0	117	1.00	0	117S
---	-----	------	---	------

Overpaid rent allowances (prior years)

DWP error overpayments recovered.

0	118	NIL	0	118S
---	-----	-----	---	------

DWP overpayments not recovered.

-355	119	1.00	- 355	119S
------	-----	------	-------	------

LA error and administrative delay overpayments.

107,764	120	NIL	0	120S
---------	-----	-----	---	------

Eligible overpayments.	306,469	121	0.40	122,588	121S
Duplicate payments.	0	122	0.25	0	122S
Recovered overpayments resulting from the use of payments on account made under Reg.93 of SI 2006 No. 213 or Reg.74 of SI 2006 No.214.	0	123	NIL	0	123S
Overpayments resulting from the use of payments on account made under Reg.93 of SI 2006 No. 213 or Reg.74 of SI 2006 No.214 which have not been recovered.	0	124	1.00	0	124S
Total subsidy claimed at full rate Cell 125S = (095S + 098S + 099S + 100S + 102S + 103S + 104S + 106S + 109S + 110S + 112S + 117S) - (118 + 120 + 121 + 122 + 123).				51,378,249	125S
Total subsidy claimed at reduced rates Cell 126S = 096S + 114S + 115S + 121S + 122S.				496,716	126S
Total rent allowance subsidy claimed Cell 127S = 125S + 126S + 210S.				52,107,472	127S
Modified scheme subsidy (This figure to be transferred from cell 216S.)				20,732	128S
Total subsidy Cell 129S = 127S + 128S (The amount in cell 129S is entered in cell 004.)				52,128,204	129S
In-year reconciliation Cell 130 = total of cells 095 to 117; this must equal the figure in cell 094.	52,784,460	130			
Backdated expenditure	6,613	131			
Cells 132 to 178 - Spare					
Subsidy additions and deductions					
Uncashed payments Subsidy reduction in respect of uncashed payments prior to 2022/2023 (The amount in cell 179S is entered in cell 006.)				0	179S
Cells 180 to 190 - Scotland and Wales					
Cells 191 to 200 - Spare					

LA error and administrative delay subsidy

Total expenditure attracting full subsidy
(Cells 034S + 073S + 125S)

53,514,217	201
------------	------------

Lower threshold (cell 201 x 0.48%).

256,868	202
---------	------------

Upper threshold (cell 201 x 0.54%).

288,977	203
---------	------------

Total LA error and administrative delay overpayments
(Cells 026 + 031 + 065 + 070 + 113 + 120)

233,230	204
---------	------------

Subsidy calculation

Enter the figure from cell 204 if less than or equal to cell 202.
Otherwise enter "0".

233,230	205
---------	------------

Enter the figure from cell 204 if more than cell 202 but less than or equal to cell 203. Otherwise enter "0".

0	206
---	------------

LA error and administrative delay subsidy due
(cell 205 + (cell 206 x 0.40)).

233,230	207S
---------	-------------

LA error and administrative delay subsidy apportionments

Rebates for non-HRA properties (cell 207S x ((cell 026 + 031) divided by cell 204)). This figure to be included in cell 036S.

723	208S
-----	-------------

Rebates for HRA properties (cell 207S x ((cell 065 + 070) divided by cell 204)). This figure to be included in cell 076S.

0	209S
---	-------------

Rent Allowances (cell 207S x ((cell 113 + 120) divided by cell 204)).
This figure to be included in cell 127S.

232,507	210S
---------	-------------

Cell 211 - Spare

Modified schemes subsidy

Total subsidy claimed before any addition in respect of the operation of a local scheme. (Cells 036S + 076S + 127S)

54,244,287	212
------------	------------

Enter 0.2% of cell 212.

108,489	213
---------	------------

Expenditure due to the **voluntary** disregarding of War Disablement Pensions or War Widows Pensions.

27,642	214
--------	------------

Enter 75% of cell 214.

20,732	215
--------	------------

Enter the lower of cells 213 and 215. This figure to be transferred to cell 128S.

20,732	216S
--------	-------------

Modified schemes

Total paid on increase in benefit arising from local schemes which allow some or all of a war disablement or war widow's pension to be disregarded.

Non-HRA Rent Rebate	HRA Rent Rebate	Rent Allowance	Total HB	
0	0	27,642	27,642	225

Local authority certificate

- * I apply on behalf of the authority for payment, in advance of certification by the Reporting Accountant, of the amount shown at cell 009.

- * I undertake on behalf of the authority to pay on demand to the Secretary of State the amount shown at cell 009.

I certify that I have examined the entries within this form and that to the best of my knowledge and belief -

the entries are accurate;

the expenditure, on which the claim is based, has been properly incurred in accordance with the Social Security Contributions and Benefits Act 1992 and the instructions made or having force thereunder, in particular the Housing Benefit Regulations 2006;

this claim for subsidy is on the form required by the Secretary of State and the information given on it is in accordance with that Act and the instruments made or having force thereunder, in particular the Income-related Benefits (Subsidy to Authorities) Order 1998;

no amounts in this claim have been included in any claim by an authority or authorities* acting as an agent or agents* of this authority; and

the authority's administrative systems, procedures and key controls for awarding benefits operate effectively and the authority has taken reasonable steps to prevent and detect fraud.

Signed : 

Date : 31/01/2024

This signature, certifying this claim, must be that of the officer responsible pursuant to Section 151 of the Local Government Act 1972 (Responsible Finance Officer)

Name (Block capitals) ASHLEY HUGHES

Position held : Director of Resources

* *Delete as necessary*

Reporting accountant: HBAP record

Further to the attached reporting accountant's report dated,
I confirm that this claim form:

- remains as the original*
- replaces the original*
- amends the original submitted*

(* please tick as appropriate)

Signature

Name (Block capitals):

Date:

Contact details:

The Subsidy Calculation

- 1.1 Local Authorities (LAs) receive, for the greater part of the qualifying benefit expenditure they incur, a direct subsidy of 100%. However, in areas of expenditure wherein LAs have most scope to monitor and control costs, lower rates apply.
- 1.2 The areas of benefit spending which attract a lower rate of subsidy are:
- certain types of overpaid benefit and duplicate payments;
 - rent rebate payments above a specified level in respect of homeless people in board and lodging, licensed and short-term accommodation;
 - rent allowance payments above a specified level in respect of temporary or short-term accommodation where a Registered Housing Association is the landlord;
 - rent allowance payments above or without the required rent officer determination.

Overpayments of Housing Benefit

- 1.3 Overpayments of Housing Benefit attract different rates of subsidy dependent on the reason for the overpayment. This is demonstrated in table one below:

Table 1:

Overpayment Type	Description	Subsidy received
Claimant error	Caused by the claimant failing to provide information or report a change in circumstances.	40%
Fraud	Where the claimant, in relation to the overpayment, <ul style="list-style-type: none"> • been found guilty of an offence; • admitted an offence in an interview under caution; or • Agreed to pay an administrative penalty. 	40%
DWP error	Arisen from a mistake by the DWP or HM and Customs	100%
Local Authority error	Arisen from a mistake by the local authority. For example, miscalculating a claim.	Various
Administrative delay	When a local authority receives all the information to make a change to a claim but delays doing so.	Various
Other	Does not fit into any of the other categories.	40%

- 1.4 The subsidy attained for Local Authority error and Administrative delay overpayments is dependent on thresholds of the total amount of these types of overpayment in relation to the full amount of correct Housing Benefit paid. This is demonstrated in table two below:

Table 2:

Percentage of amount of Local Authority error and Administrative delay overpayments	Subsidy received
Less than or equal to 0.48% of correct amount of Housing Benefit paid	100%
Greater than 0.48% but less than or equal to 0.54% of correct amount of Housing Benefit paid	40%
Greater than 0.54% of correct amount of Housing Benefit paid	0%

- 1.5 The subsidy for overpaid Housing Benefit is paid regardless of whether the Council recover the amount overpaid. It is essential that recovery of overpayments is maximised as it can be financially beneficial to the Council as in the following example:
- Housing Benefit paid out £100.00
 Claimant error overpayment of £100.00 recovered in full from the claimant.
 Subsidy received from the DWP £40.00
 The Council keep the £40.00 in addition to the amount covered by subsidy before the overpayment is recovered.

1.6 The subsidy claimed for overpaid Housing Benefit can be found in cells 024 to 033S, cells 111 to 124S and cells 201 to 210S of the statement at Appendix One.

Temporary accommodation and board and lodging

1.7 These subsidy rates apply to Housing Benefit paid for accommodation provided by a local authority, or a registered housing association, as temporary or short-term accommodation. An example would be where the accommodation has been made available by the local authority to discharge a statutory homeless function.

1.8 For self-contained accommodation, the subsidy is based on the size of the property. A self-contained property is where the claimant's household is not required to share a kitchen, bathroom and toilet. This type of property attracts subsidy at a rate of 90% of the Local Housing Allowance Rate, set in January 2011, for the number of bedrooms in the property.

1.9 Housing Benefit paid for properties providing board and lodging attracts subsidy of the Local Housing Allowance Rate, set in January 2011, for one bedroom.

1.10 Any expenditure above those rates will not attract any subsidy and has to be funded by the Council. It is therefore vital that Homelessness Services consider spend when placing homeless residents in accommodation.

1.11 The subsidy claimed for temporary accommodation and board and lodging can be found in cells 012 to 023S of the statement at Appendix One.

Rent Allowance Payments

1.12 New Housing Benefit claims made after 07 April 2008 are based on the Local Housing Allowance rate for the property.

1.13 Entitlement to Housing Benefit in certain circumstances, however, are not subject to the Local Housing Allowance rate. This includes:

- Registered Social Landlords
- Regulated tenancies
- Pre 1996 cases
- Maximum rent cases
- Exempt and Supported accommodation
- Caravans, houseboats, mooring fees, mobile homes, hostels
- Board and lodging

1.14 The rents for Registered Social Landlords are normally accepted as being market value, however, the rent can be deemed by the local authority to be excessive.

1.15 Claims that fall within these categories require a Market Rent assessment by the independent Rent Officer Services. Subsidy will only be paid at the rate set by the Rent Officer and any Housing Benefit paid in excess of that amount will be met by the Council.


1.16 The subsidy claimed for rent allowance claims can be found in cells 094 to 110S of the statement at Appendix One.

Modified Schemes

1.17 The Executive Cabinet approved, on 27 September 2023, a modified scheme for Housing Benefit allowing the whole of any prescribed war disablement pension or prescribed war widow's pension payable to that person to be disregarded as income. The Council receive 75% subsidy on the additional Housing Benefit payable due to this income disregard.

1.18 The subsidy claimed for rent allowance claims can be found in cells 212 to 216S of the statement at Appendix One.

Report To:	AUDIT PANEL
Date:	12 March 2024
Reporting Officer:	Elizabeth McKenna and Nichola Cooke
Subject:	STAR PROCUREMENT UPDATE – TAMESIDE COUNCIL
Report Summary:	The report located at Appendix 1 provides an update for Audit Panel on the performance of STAR including procurement activity for Tameside Council, compliance, and collaboration opportunities. The report outlines the work undertaken through the Collaborative Audit Group and details how STAR manages procurement risks. The report also details STAR's plans for further development.
Recommendations:	For Audit Panel to note the work of STAR Procurement, its performance and plans for further development.
Links to Corporate Plan:	Efficient and effective procurement supports the priorities within the Corporate Plan.
Policy Implications:	Effective procurement supports the policy objectives of the Council.
Financial Implications: (Authorised by the statutory section 151 Officer & Chief Finance Officer)	Effective procurement helps ensure best use of Council's assets, ensure Value for Money and support good governance.
Legal Implications: (Authorised by the Borough Solicitor)	<p>There are no immediate legal implications arising from this update report.</p> <p>STAR provides a critical support to ensure that procurement exercises are undertaken compliantly and also deliver best value for the council.</p> <p>Ongoing oversight of STAR ensures that performance is monitored and that all opportunities such as collaborations are explored particularly in the challenging economic climate.</p>
Risk Management:	Effective procurement minimises a range of risks, financial, legal, and reputational.
Access to Information:	The background papers relating to this report can be inspected by contacting Elizabeth McKenna, Assistant Director, STAR Procurement.

 07811 985687/ 07711 454555

 elizabeth.mckenna@star-procurement.gov.uk
Nichola.cooke@star-procurement.gov.uk

This page is intentionally left blank

Report to: Tameside Audit Panel
Date: 12th March 2024
Report of: Assistant Director (Delivery), STAR Procurement

STAR Procurement Update – Tameside Council

1. Background

STAR Procurement was 10 years old in February 2024, and is now a six-partner shared service as St Helens Council and Knowsley Council joined the shared service in October 2023. The addition to the shared service brought with it 11 TUPE staff to enhance the STAR team and deliver a robust procurement service to all six partners.

STAR is the internal procurement team for Tameside and the other five Councils and operates as a formal collaborative service governed by a Joint Committee with equal representation from each of the six partner authorities.

STAR continues to deliver the Core Offer to its partner authorities and provides collaborative strategic leadership, management and operational support, advice, and guidance to all officers for all procurement and facilitates procurement activity over £25k. STAR delivers on the Responsible Procurement Strategy [Ethical & Sustainable Procurement \(star-procurement.gov.uk\)](https://star-procurement.gov.uk) as well as the Business Plan [Business Plan \(star-procurement.gov.uk\)](https://star-procurement.gov.uk). The Business Plan expires in 2024 and STAR Leadership Team, STAR Board and Joint Committee are working on a review of the business plan ready for a launch of a new Procurement Strategy later in the year.

2. Procurement Activity in 22/23 Compliance and Collaboration:

2.1 Activity:

In 22/23 STAR undertook 125 procurements for Tameside Council.

These consisted of:

- 18 Above Threshold Tenders (Above the Public Procurement Regulation Value Thresholds for Goods and Services £213,477K and for Works £5,336,937)
- 31 Call off from a Framework/direct award (These are compliant routes to market)
- 19 Exemptions, this is where a Tameside officer wishes to utilise the Council's Constitution rules (CPRs - Contract Procedure Rules) to directly award/extend a contract without competition, exemptions must be approved by Tameside legal team
- 53 Below Threshold Low Risk Procurements (Risk Based Sourcing)
- 4 Below Threshold High Risk Procurements (Risk Based Sourcing)

Historical Data

	18/19 Part Year	19/20	20/21	21/22	22/23
Above FTS Threshold	0	15	12	11	18
Framework Call offs	9	23	34	31	31
Exemptions	1	15	25	14	19
Low Risk RBS	9	60	40	38	53
High Risk RBS	16	2	12	6	4
Total	35	115	123	100	125

The volumes of work will fluctuate year on year depending on contract end dates, the general trend is more work is now being undertaken by STAR, particularly for above Find a Tender Threshold and Risk based Sourcing activities. Tameside joined STAR part way through the financial year in 18/19.

2.2 Compliance:

Utilising spend data from Tameside's finance system, STAR officers review all third party spend against the STAR Contract Register (Intend); if the spend/supplier is on the Contract Register, the spend is marked as compliant spend. Any spend/supplier that is not identified on the Contract Register is marked as non-verified spend and STAR officers work with budget holders/commissioners to ensure compliance is secured either by adding contract to the contract register or planning the appropriate procurement. This is a rolling programme, and the position isn't ever static.

Tameside Performance on Compliance:

- 22/23 Tameside Council have 89.1% of third party spend on the contract register.
- When Tameside joined STAR in 18/19 compliance was 81%.
- The 22/23 compliance figure for STAR is 92.2% and so Tameside were positioned below the STAR average at the end of 22/23.
- There is some targeted work continuing in 23/24 within Tameside to drive improvement for compliance.
- Targeted work has taken place to ensure there are accurate 5-year pipeline plans produced via Intend (systemised).
- Over the last twelve months quarterly data weeks have been diarised with category managers to focus on compliance and non-verified spend, this is in addition to the standard data month processes that already take place.
- STAR attends the Assistant Directors Delivery Group (ADDG) meetings to ensure any issues or problems are discussed and resolved.
- STAR have had zero legal challenges for any of the STAR partners.

2.3 Collaboration:

In March 2023 STAR launched 'Collaboration First' which is a focussed programme of reviewing the procurement pipeline to identify collaborative opportunities across the STAR partners as well as regionally which will bring efficiencies from being a bigger buyer which will in turn provide resource efficiencies. In 23/24 STAR are setting a benchmark of collaboration data with a view to Joint

Committee setting a collaboration target in 24/25. Regular updates on progress are provided to STAR Board and Joint Committee.

2.4 Collaborative Audit Group:

STAR work closely with the six Chief Auditors across the six STAR partner authorities, with a quarterly meeting to agree the shared audit plan. Bringing in the fifth and sixth partner to STAR has brought efficiencies for Tameside Audit team as previous STAR audits were split between the four partners and now split between six partners, in addition to enhancing the knowledge sharing between the six audit teams.

Audits undertaken in 22/23 and 23/24:

1. Income Audit (In Progress)

Tameside delivery auditing STAR income and invoicing

2. Risk Based Sourcing Audit

Trafford delivery auditing the STAR approach to Risk Based Sourcing

Outcomes:

- Use the contract criticality tool to ensure risk was assessed more scientifically.
- Roll out refresher training for all staff on market engagement and Procurement Initiation Document (PID) completion.

3. Intend Audit

Stockport Delivery auditing the Contract Register System and utilisation of the Contract Management Tool

Outcomes:

- Contract Management group set up for STAR Partners.
- Further developed training and guidance documentation.
- Created a contract criticality tool and graded all contracts.
- Regular meetings now take place with the Intend account manager.

4. Contract Extensions (in progress)

Rochdale Delivery auditing compliance with Contract Procedure Rules and governance on Contract Extensions

The current shared Audit Plan includes:

- Social Value Delivery
- New Procurement Regulations implementation
- Supply Risks
- Real Living Wage

Tameside are currently undertaking the income audit, the audit function is rotated across the six STAR Partners, so Tameside will not be directly involved in any of the audit plans next year, but results from the audits will be circulated to all STAR Partners.

3. Performance:

22/23

£571,072 efficiencies

22.4% Social Value return secured on total contract value, accumulative over the past 4 years.

49.4% spend retained within Tameside.

74.7% spend retained within Greater Manchester.

Historical Data

	18/19	19/20	20/21	21/22	22/23
Efficiencies (£)	Part Year	1,900,029	2,975,716	957,950	571,072
Social Value Return (%)	Part Year	19.5	18.9	25.0	22.4
Local spend-Tameside (%)	53.0	62.0	67.8	53.6	49.4
GM Spend	70.0	68.0	62.3	75.2	74.7

The trends in this table demonstrates an increase in Social Value and although local spend is decreasing the GM spend is increasing and efficiencies are on a downward trajectory. Efficiencies is a focus for STAR and Tameside officers, working together to plan, record and implement procurement efficiencies to increase the capture and delivery of revenue efficiencies.

4. Continuous Improvement for STAR and its Partners:

STAR has a Continuous Improvement (CI) group which has representatives from each of the six STAR partner authorities. This helps us to drive improvement and challenge process and practice. This is reported quarterly to STAR Board and Joint Committee.

The focus of the CI Group is the New Public Contract Regulations which are expected to come into force in October 2024, there is a Task and Finish Group set up with representatives from each partner authority to collectively work on the effect that the new regulations will have on procedures and processes within each partner authority. The regulations come with them a requirement for more transparency in particularly around contract management, the Task and Finish Group are exploring what that will mean for each partner authority and will be reporting directly to the Assistant Directors Delivery Group on any changes required.

Continuous Improvement Update for STAR and Tameside:

Since the last report to Audit Panel STAR has worked closely with the Assistant Directors Delivery Group (ADDG) within Tameside and improved relationships between procurement and officers within directorates, working with ADDG monthly has improved communication and regular sharing of pipeline as well as improved the process around Exemptions and Modifications and any blockages in the system are dealt with quicker. There are further improvements planned to implement online forms for Procurement Initiation Documents (PIDs), Exemptions and Modifications which is due to launch in April 2024.

5. **Risk**

STAR utilises the Three Lines of Defence Model for managing risk, examples of the potential risks that STAR consider whilst delivering the shared procurement service are:

Potential Risks

Budget pressures	Market Conditions	Climate Emergency
Global Financial Crisis	Market Stability	GM Employment Charter/RLW
Modern Slavery	Regulation/Policy changes	Specific Project Risks
S114 Risk	STAR SLA's	
Moratorium on Spend	Complexity of Documents	

Managing Risks

First Line:

- STAR has Management Controls including escalation within the STAR structure, via the STAR Board representative for Tameside, Ashley Hughes, then up to STAR Board then STAR Joint Committee.
- STAR also have Internal Control Measures such as being the 'gatekeeper' on procurement governance for each partner authority, a robust Quality Management System, continuous training offer, regular communication within STAR and partner authorities, regular reporting, analysing, monitoring data and robust escalation processes.

Second Line:

- STAR facilitates Financial Control by including checks on budget availability for procurement within processes, assessing supplier/contractors at tender stage and STAR utilise the Trafford Finance SLA for the management of the STAR budget.
- Security includes upholding the integrity/availability/confidentiality of each partner authority's data, adhering to data sharing protocols STAR utilise the Stockport Data SLA for STAR data and the whole STAR team complete annual GDPR training via Trafford Council as host authority.
- Risk management is monitored via the STAR Risk Register which supports the Corporate Risk Registers within each partner authority. In addition, STAR have support from the STAR Legal team which is an SLA with Trafford's legal service.
- Quality is managed through the PID requirement, regular assessments from colleagues and Board members from each partner authority to ensure that STAR is of an appropriate quality and feedback from users of the STAR service both internally and externally to improve services, this is in addition to the cross-partner Continuous Improvement Group described earlier in the report.
- STAR governance has been inspected by external experts to ensure efficiency and effectiveness, STAR had a legal review in 2022 by Trowers and Hamlin to ensure that the STAR trading and income activity was robust.
- Compliance is reported and monitored by STAR Board and Joint Committee.

Third Line and External:

- Collaborative Audit Group has a joint plan for 6 partner authorities.
- STAR contribute to the Annual Governance Statement where required.
- STAR engage with External Audit when required.

- STAR influence and manage external factors including Procurement Regulations, relevant National Policy and Strategy requirements, implement Procurement Policy Notices (PPNs).
- STAR report quarterly to STAR Board, STAR Joint Committee on emerging risks and present an annual risk register.
- STAR attend Audit Committee annually and attend Cabinet and Scrutiny Committee when required.

6. Recommendations

To note the work of STAR Procurement, its performance and plans for further development.