Public Document Pack

Leeds
CITY COUNCIL

CORPORATE GOVERNANCE AND AUDIT COMMITTEE

Meeting to be held in Civic Hall, Leeds, LS1 1UR on
Monday, 12th February, 2024
at 10.30 am

MEMBERSHIP

Councillors

G Almass
J Dowson
H Bithell
M France-Mir (Chair)
J Heselwood
P Wray

C Hart-Brooke

S Firth
M Robinson

Independent Member

L Wild

Please do not attend the meeting in person if you have symptoms of Covid 19 and please follow current public health advice to avoid passing the virus onto other people.

We strive to ensure our public committee meetings are inclusive and accessible for all. If you are intending to observe a public meeting in-person, please advise us in advance by email (FacilitiesManagement@leeds.gov.uk) of any specific access requirements, or if you have a Personal Emergency Evacuation Plan (PEEP) that we need to take into account. Please state the name, date and start time of the committee meeting you will be observing and include your full name and contact details.

Note to observers of the meeting. To remotely observe this meeting, please click on the 'View the Meeting Recording' link which will feature on the meeting's webpage (link below) ahead of the meeting. The webcast will become available at the commencement of the meeting: Council and democracy (leeds.gov.uk)

Agenda compiled by: Debbie Oldham
Governance Services
Civic Hall

AGENDA

Item No	Ward	Item Not Open		Page No
1			**APPEALS AGAINST REFUSAL OF INSPECTION OF DOCUMENTS** To consider any appeals in accordance with Procedure Rule 15.2 of the Access to Information Procedure Rules (in the event of an Appeal the press and public will be excluded). (*In accordance with Procedure Rule 15.2, written notice of an appeal must be received by the Head of Governance Services at least 24 hours before the meeting)	
2			**EXEMPT INFORMATION - POSSIBLE EXCLUSION OF THE PRESS AND PUBLIC** 1 To highlight reports or appendices which officers have identified as containing exempt information, and where officers consider that the public interest in maintaining the exemption outweighs the public interest in disclosing the information, for the reasons outlined in the report. 2 To consider whether or not to accept the officers recommendation in respect of the above information. 3 If so, to formally pass the following resolution:- **RESOLVED –** That the press and public be excluded from the meeting during consideration of the following parts of the agenda designated as containing exempt information on the grounds that it is likely, in view of the nature of the business to be transacted or the nature of the proceedings, that if members of the press and public were present there would be disclosure to them of exempt information, as follows:-	

Item No	Ward	Item Not Open		Page No
3			**LATE ITEMS** To identify items which have been admitted to the agenda by the Chair for consideration (The special circumstances shall be specified in the minutes)	
4			**DECLARATION OF INTERESTS** To disclose or draw attention to any interests in accordance with Leeds City Council's 'Councillor Code of Conduct'.	
5			**APOLOGIES FOR ABSENCE**	
6			**MINUTES OF THE PREVIOUS MEETING - 27TH NOVEMBER 2023** To receive the minutes of the meeting held on 27th November 2023, for approval as a correct record.	7 - 16
7			**MATTERS ARISING FROM THE MINUTES**	
8			**ANNUAL ASSURANCE REPORT OF INFORMATION DIGITAL SERVICES (IDS) GOVERNANCE.** The annual report of the Chief Digital and Information Officer to the Committee concerning the decision-making arrangements within the Integrated Digital Service (IDS) and provides assurances that these arrangements are up to date, fit for purpose, effectively communicated and routinely complied with.	17 - 48

Item No	Ward	Item Not Open		Page No
9			**ANNUAL INFORMATION GOVERNANCE REPORT, INCLUDING THE ANNUAL REPORT OF THE CALDICOTT GUARDIAN** This annual report of the Director of Strategy and Resources and Director of Adults and Health presents assurances to the Corporate Governance & Audit Committee on the effectiveness of the council’s information management and governance arrangements through a statement of internal control. In addition, the report this year presents the Information Commissioner's Office (ICO) Audit Report of Leeds City Council’s compliance with the UK General Data Protection Regulation (GDPR).	49 - 122
10			**INTERNAL AUDIT UPDATE REPORT** The report of the Chief Officer Financial Services provides a source of assurance that the internal control environment is operating as intended through a summary of the Internal Audit activity for the period from September to December 2022. The report highlights the incidence of any significant control failings or weaknesses.	123 - 156
11			**COUNTER FRAUD UPDATE REPORT APRIL - DECEMBER 2023** The report of the Senior Head of Audit, Corporate Governance and Insurance provides a source of assurance that the internal control environment is operating as intended through a summary of the counter fraud activity for the period from April to December 2023.	157 - 188

Item No	Ward	Item Not Open		Page No
12			**UPDATE REPORT ON GOVERNMENT PROPOSALS TO ADDRESS THE NATIONAL AUDIT BACKLOG, AND GRANT THORNTON'S RESPONSE AND UPDATE ON THE AUDIT 2021/22** The report of the Chief Finance Officer informs Members of the Government’s most recent proposals to address the backlog of incomplete audits across local government in England. Grant Thornton’s accompanying report sets out their intended approach in response to the Government’s proposals, should these go ahead. The report also provides a summary update on the progress towards completing the audit of the 2021/22 statement of accounts.	189 - 192
13			**CORPORATE GOVERNANCE AND AUDIT COMMITTEE WORK PROGRAMME 2023-24** This report presents the work programme for the Corporate Governance and Audit Committee, setting out future business for the Committee’s agenda, together with details of when items will be presented.	193 - 198
14			**DATE AND TIME OF NEXT MEETING** To note the next meeting will be on Monday 18th March 2024, at 10.30am.	

Third Party Recording

Recording of this meeting is allowed to enable those not present to see or hear the proceedings either as they take place (or later) and to enable the reporting of those proceedings. A copy of the recording protocol is available from the contacts named on the front of this agenda.

Use of Recordings by Third Parties– code of practice

a) Any published recording should be accompanied by a statement of when and where the recording was made, the context of the discussion that took place, and a clear identification of the main speakers and their role or title.
b) Those making recordings must not edit the recording in a way that could lead to misinterpretation or misrepresentation of the proceedings or comments made by attendees. In particular there should be no internal editing of published extracts; recordings may start at any point and end at any point but the material between those points must be complete.

This page is intentionally left blank

Corporate Governance and Audit Committee

Monday, 27th November, 2023

PRESENT:	Councillor M France-Mir in the Chair
	Councillors G Almass, J Dowson, H Bithell, C Hart-Brooke, J Heselwood, P Wray, S Firth and M Robinson
INDEPENDENT MEMBER:	L Wild

41 Appeals Against Refusal of Inspection of Documents

There were no appeals against refusal of inspection of documents.

42 Exempt Information - Possible Exclusion of the Press and Public

There were no exempt items.

43 Late Items

With the permission of the Chair items had been added to the agenda in relation to Grant Thornton Annual Report 2022/23 and Grant Thornton Updated Interim Audit Findings Report 2021/22. It was noted that these would be taken as Agenda Items 13 and 14.

44 Declaration of Interests

No declarations of interests were made at the meeting.

45 Apologies for Absence

There were no apologies.

46 Minutes of the Previous Meeting- 25th September 2023

RESOLVED – That the minutes of the meeting held on 25th September 2023, be approved as a correct record.

47 Matters Arising From The Minutes

There were no matters outstanding.

48 Procurement Assurance Report 2022-23

The report was presented by the Head of Procurement and Commercial Services.

The Committee were informed of the following points:

- It was noted that the report for 2022/23 was the same as last year with high inflation and increased demand for services. Members were advised that compliance was still strong and there were no issues to report.
- Members noted that the arrangements for procurement were still robust, and advice was provided to services.
- Council's Contract Procedure Rules (CPR's) which are reviewed each year were currently undergoing a comprehensive refresh as part of a broader review of the Council's Constitution with a view to simplifying and making them more user friendly.
- The Committee were advised that spend for local suppliers and SME's was slightly down on the previous year. Members were informed that new recruits had been appointed to assist with all aspects of Social Value activity.
- It was noted that the P2P Review was still ongoing.

Responding to questions from Members the following information was provided:

- The Committee were advised that any spend over £10,000 is published to the register on YORtender. It was noted that at present 6 contracts were not currently on YORtender. Progress was monitored, and this information could be sent to the Committee.
- Members noted that Equality, Diversity and Inclusivity (EDI) were taken into account in relation to Social Value contracts. Members were advised that waivers were only used in exceptional circumstances. The Committee were informed that the operational service was responsible for contract management, budget, and service provision, however, advice and assistance was provided by The Procurement and Commercial Service if required.
- The Procurement and Commercial Service provided training and awareness courses.
- The Committee were informed that the Council can hold providers and suppliers to account for poor performance and service.
- Information in relation to Go4Growth was not available at the meeting but would be provided to the Committee.
- In relation to local suppliers, it was acknowledged that work was required to liaise with the local market, so they were aware that they can contract with the Council. The Committee requested a briefing paper on how the service plans to communicate with the local market so that the Council has assurance that it is comfortable with the process for communication. It was recognised that communication was used effectively and that there was a need to cast the net wider.
- The Committee noted that local suppliers come from Leeds and the West Yorkshire region.
- The Committee noted that a report in relation to Social Value was due to go to the relevant Scrutiny Board in the New Year.

- Confirmation was given that the P2P Review was still ongoing as per recommendations of the LGA Peer Review. This would form part of the overall Core Business Transformation Programme.
- It was recognised that as part of the Internal Control different questions had been used from the previous year. It was noted that Contract Management had improved across the Council, Information on the questions used this year and in previous years would be checked and provided to the Committee.
- Members were advised that the CPR's would be ready by the end of the financial year and would be user friendly. It was noted that officers had capabilities to manage contracts and were updated through the newsletter, training, and awareness courses and any through appraisal system.
- When contracts are in place they are monitored and reviewed some on a quarterly basis or annually with the service.

RESOLVED – To:

a) Consider and note the assurances provided in the report from the review, assessment, and on-going monitoring.
b) Note that the Head of Procurement and Commercial Services has reached the opinion that procurement policies and practices are up to date, fit for purpose, and effectively communicated.
c) Note the ongoing P2P Review.

49 Annual Assurance Report on Corporate Performance Management Arrangements

The report of the Director of Strategy and Resources presented assurance to the Committee on the effectiveness of the Council's corporate performance management arrangements.

The Committee were provided with the following information:

- The introduction of the Best City Ambition, adopted by full Council in February 2022, had necessitated a review of the performance framework and the KPI'S routinely reported to CLT, Executive Board and Scrutiny.
- Following transitional arrangements introduced for 2022/23, a single list of KPI's is being refined through discussions with services and scrutiny chairs to ensure there are appropriate measures to routinely monitor and measure the Council's performance. It was noted that associated systems and processes are also being reviewed at the same time to ensure efficiency and robustness.
- The Committee were advised that Oflog had outlined a list of KPI's for which the Council will be required to submit data.

Responding to questions from the Members the Committee were provided with the following information:

- These performance indicators look at performance at a high level it would only be indicators such as repairs indicators that would be investigated to a lower level. Corporate and personal performance indicators are used to look at performance of the workforce and individuals, this is done through Health and Safety, Appraisals and the Strategy and Resources Scrutiny Board. Extra provision is provided at a local level for personal performance using the 'Golden Thread' approach of top to bottom and bottom to top framework which is complex. Where issues are identified these are dealt with through the appraisal system. It was noted that there had been positive feedback from the staff survey.

- The KPI's will inform CLT by identifying any issues and raised for discussion at relevant meetings. Services and Directorates raise matters about areas where improvement is required and report on any actions being taken to address falling performance.
- It was noted that the Survey of Internal Control had shown that performance management was 'well embedded' by 93% of respondents. The Committee were informed that the questions in the survey had been slightly different to the previous years' questions. It was acknowledged that this was a wider ranging review with services and conversations with Scrutiny Board Chairs.
- Benchmarking analysis is provided within the performance report. Comparisons with other core cities is used and most services are well established for benchmarking data. The data is fed into CLT.
- In relation to the Contact Centre KPI's any key issues are fed through to CLT. It was noted that comparisons for previous years was needed.
- It was recognised that the list of indicators from Oflog would provide some uniformity. It was noted that these would be reported to Oflog on an annual basis.
- The Committee requested comparative information for year on year from the Survey of Internal Control.
- Members were advised that a report was due to Scrutiny in relation to the Contact Centre, but the Council was waiting for Oflog to provide guidance on what would be required.
- The Committee noted that the HR assurance report would be coming to this Committee in March 2024.

RESOLVED – To receive the report and the attached Appendix 1 as together providing key forms of assurance on the robustness of the authority's corporate performance management arrangements.

50 Annual Assurance Report on Risk and Resilience Arrangements

The report of the Director of Strategy and Resources provided the Committee with assurances relating to the adequacy of the risk and resilience controls currently in place in the Council.

The Committee were informed of the following points:

- Risk and resilience cover three inter-related areas of Risk Management, Emergency Planning and Business Continuity Management. This is at Corporate, Directorate and operational level.
- The service works with a wide range of stakeholders and attends a number of boards and team meetings to discuss risk and resilience matters.
- There has been an increased demand in risk training given the new challenges and new risks.
- Following a recent exercise to compare the strategic risks on Core Cities risk registers, key contacts from the local authorities will be meeting regularly to discuss risk management including best practice, emerging risks and lessons learned which will be useful going forward.
- Following a recent Internal Audit review of our risk management arrangements, we will be documenting lessons learned from the Internal and external sources in relation to risk. This will enable us to provide more evidence that any lessons learned are being considered.
- In relation to Appendix 2 it was noted that this is the same as last year with the level of engagement positive and fully embedded.
- Resilience emergency planning is publicly available and on the Council's website.
- X formerly known as Twitter is used to communicate on a number of issues including adverse weather conditions, incidents, awareness campaigns and pollution alerts.
- The service has a link to the National Power Grid to be alerted of power outages.
- An induction session had been provided to Members in May 2023, and the service had delivered sessions in Autumn and there was also one scheduled for January 2024. Training had also been delivered to the Community Committee Chairs Forum. Members were also advised of training sessions which included role play for emergency evacuation and setting up of reception centres. It was noted that the Council had received a Gold Paw Print Award for this.
- An event had taken place to re-launch the Business Continuity Network which had focused on Martyn's Law which had been part of the King's Speech at Parliament. This event is to be a bi-annual event going forward.
- Audit had highlighted weaknesses in business continuity awareness and training. Therefore, the service is assessing business continuity plans and will be addressing any weaknesses through training and awareness courses, to ensure robust planning and to meet legislative duty.

Responding to questions from the Members the Committee were provided with the following information:

- It was acknowledged that the risk map has a large focus on financial issues which included staffing. The risk map is reviewed by Corporate Leadership Team on a regular basis. It was recognised that the Council cannot be risk averse as there is a need to take some risks, but they need to be regularly reviewed and managed.

- The Committee were advised that work was ongoing with IDS to address risk appetite and tolerance levels on IT issues including cyber risk. It was noted that training was required in this area.
- It was acknowledged that financial risks effect all parts of the Council, but the Council has a robust Financial Strategy and where areas of risk are identified they are reviewed, and RAG rated. Transformation teams support implementation of any actions that are required.
- Members requested information on risk trends for future meetings.
- It was noted that on resilience day exercises a code word is built into the exercise which would send an alert that a real incident had occurred and stop the exercise.
- It was noted that in December the service is due to meet with colleagues in IDS to draw up a plan should a major incident occur.
- Members were advised that new updates were required for continuity plans. Next year members of the community were to come together with the service to draw up robust local area plans.

RESOLVED - To receive the annual report on the Council's risk and resilience arrangements and note the assurances in support of their next Annual Governance Statement.

51 Annual Assurance report on Financial and Treasury Management

The report of the Chief Officer Financial Services set out the standing arrangements for financial management and treasury management within the Council and provided evidence of compliance over the reporting period from November 2022 to October 2023.

The Committee were informed of the following points:

- It was noted that this report fulfilled the Chief Finance Officers Protocol which forms part of the Council's Constitution to report to the Committee on an annual basis.
- Members were informed that given the financial challenges that the Council faces as set out in the medium and long term financial strategy it is appropriate that the Council has appropriate financial and treasury management arrangements in place.
- The treasury management governance is appropriate, and the Council is operating within its governance framework and as such is complying with the CIPFA Treasury Management Code of practice, Prudential Code and updated guidance notes.
- It was noted that the report was similar to previous years as it describes democratic and officer oversight of financial arrangements and framework as set out in the Constitution and details documents that are used and the key processes.
- The changes were highlighted as being:
    - Oflog changes which were level of reserves, level of debt of the authority and referenced in performance indicators.

- Replacement of FMS, with Microsoft Dynamics being implemented in the new financial year 2024/25.
- In terms of independent scrutiny, the report picked up key findings of the Grant Thornton 2021/22 report. It was acknowledged that this part of the report would be superseded by an updated report from Grant Thornton.

In response to questions from the Committee the following information was provided:

- Clarification was provided to Members on how the survey of internal control was approached and it was noted that there was 97% response rate.
- It was confirmed that stocks and stores would be tied into the new finance system.
- It was noted that the Chief Officer Financial Services meets with external auditors Grant Thornton on a monthly basis to review progress on the delivery of a balanced budget position and actions being taken to deliver a sustainable financial position for the years covered by the current approved Medium Term Financial Strategy. The Chief Officer also reports to Executive Board monthly and the financial position is also discussed at Scrutiny.

RESOLVED – To note the Chief Officer Financial Services assurances that:

a. In respect of both Financial Management and Treasury Management that appropriate systems and procedures are in place to ensure that there is sound financial management and control across the Authority; and
b. The arrangements set out in the Chief Finance Officer protocol have been complied with.

52 Grant Thornton Receipt of External Auditors ICT Report

The report of the Chief Finance Officer presented Grant Thornton's IT Audit Report for the 2022/23 financial year. The Auditor's report was attached at Appendix 1.

The Committee were informed that there were some issues, and these had been expanded on under the recommendations within the report. It was noted that one of the recommendations related to user administration arrangements for the financial ledger. However, officers had reviewed the current arrangements and were satisfied that they are appropriate for the existing system. The service is in the process of introducing a new financial management system and the future user administration arrangements would be specific to it, and different from those needed for the old system.

Members noted that there was no material impact on the accounts.

RESOLVED – To receive the IT Audit Report presented by Grant Thornton and to note the recommendations which have been made.

53 Grant Thornton Annual Report 2022/23

The report of the Chief Finance Officer presented Grant Thornton's Annual Auditors Report for 2022/23.

The Annual Report gave the audit findings relating to the Council's value for money arrangements. It was noted that the report did not identify any statutory recommendations but did make two key recommendations and a number of other recommendations for improvement.

Grant Thornton's Annual Report was appended to the report at Appendix 1.

The external auditors presented the Annual Report 2022/23, providing the following information:

- The value for money audit had looked at wider issues this year whilst consider if the Council had put in place proper arrangements to secure economy, efficiency and effectiveness in its use of resources.
- It was noted that on page 9 of the supplementary information pack there was a summary of findings including 2 key issues, with a number of recommendations listed.
- The auditor highlighted page 11 of the pack which related to Governance and Improving economy, efficiency and effectiveness. It was recognised that nationally this was a challenging area linked to Government funding, overspend and off set against resources. It was acknowledged that the Chief Officer was aware of the challenges and what the Council needed to do.
- There were seven recommendations across themes.

The Chief Finance Officer informed the Committee that there were two key recommendations and the Council had already done some work around improvements. It was recognised that Reserves needed to be built up over a few years and the Council has had a managed approach to raise these over the last few years. It was acknowledged that the Council was not the only one to face the challenges outlined, and that this was a national issue for local authorities.

The Committee were informed that increased social care costs in Children's Services had been built into the budget and the latest projection for the current year was due to go to Executive Board in December.

It was noted:

- The Council had clear and robust financial plans.
- The function of asset management was in a good position.
- Improvements would be delivered through the new financial management system.
- There had been challenges for the service with a number of audits all at once.

RESOLVED – To receive the Annual Auditor's Report presented by Grant Thornton and to note the recommendations which have been made.

54 Grant Thornton Updated Interim Audit Findings Report 2021/22

The report of the Chief Finance Officer presented an update Grant Thornton's Interim Audit Findings Report for their audit of the Council's 2021/22 statement of Accounts. Their report was attached as Appendix 1.

The external Auditors presented their report explaining that the updates since the previous report had been presented in blue text in Appendix 1.

It was noted that the external auditors were working with officers in Finance to resolve the 2021/22 audit of the accounts as soon as possible.

Responding to a question from the Committee it was noted that in relation to the group account disclosure, the Finance Team would be looking to expand the disclosure in the final version in the 2021/22 statement of accounts.

RESOLVED - To receive the Interim Audit Findings Report presented by Grant Thornton and to note the recommendations made.

55 Corporate Governance and Audit Committee Work Programme 2023-24

The report of the Chief Officer, Financial Services presented the work programme for the Committee, setting out future business for the Committee's agenda, together with details of items to be presented.

Members were advised that moving forward there would be a survey to the Committee.

The Chair asked Members to email her with any additional items they may wish to consider at future meetings.

RESOLVED – To consider and approve the work programme and meeting dates at Appendix A.

CHAIRS CLOSING COMMENTS

The Chair wished the Members of Committee a Merry Christmas.

56 Date and Time of Next Meeting

RESOLVED – To note that the next meeting of Corporate Governance and Audit Committee is scheduled for Monday 5th February 2024 at 10.30am.

This page is intentionally left blank

Leeds
CITY COUNCIL

Agenda Item 8

Report author: Andrew Byrom

Tel: 0113 37 84339

Decision Making Statement of Internal Control

Date: 1st November 2023

Report of: Chief Digital and Information Officer

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

What is this report about?

Including how it contributes to the city's and council's ambitions

- This is the annual report to the Committee concerning the decision-making arrangements within the Integrated Digital Service (IDS) and provides assurances that these arrangements are up to date, fit for purpose, effectively communicated and routinely complied with.
- The arrangements set out provide a framework for transparent and accountable decision making within IDS in accordance with the Council's Corporate Governance Code and Framework.
- The 100% Digital Leeds has been recognised as one of the most successful, high-profile, and well-respected digital inclusion programmes in the country by the The King's Fund, The British Academy, The Fabian Society, Local Government Association and NHS England.

Recommendations

a) Members are requested to:

   i. consider and note the positive assurances set out in the IDS Statement of Internal Control attached as Appendix A to this report;

Why is the proposal being put forward?

1 This is the annual report to the Committee concerning IDS's decision making arrangements.

What impact will this proposal have?

Wards affected:

Have ward members been consulted? ☐ Yes ☒ No

2 The report provides an assurance of the effectiveness of the arrangements for internal control within IDS which the Committee is able to consider.

What consultation and engagement has taken place?

3 The recent survey of internal control has enabled the council’s managers to reflect on their experience of the controls relating to decision making, to identify strengths and weaknesses, and to recommend solutions and draw attention to potential opportunities to improve arrangements. Details are set out in the review and refine section of the appendix to this report.

What are the resource implications?

4 The systems and processes in place to meet the requirements of the decision making framework do so from within existing resources.

5 The Statement of Internal Control confirms that arrangements ensure proportionate use of resource to secure open and accountable decision making.

What are the legal implications?

6 The IDS decision making framework meets the statutory requirements in relation to decision making and monitoring of relevant performance indicators ensures compliance.

7 The IDS Statement of Internal Control confirms that arrangements have been correctly applied and meet the statutory and constitutional framework.

What are the key risks and how are they being managed?

8 The positive assurances set out in the IDS Statement of Internal Control show that the decision making framework is fit for purpose, embedded and routinely complied with so there are no risks identified by this report in need of action over and above the described control framework.

Does this proposal support the council’s three Key Pillars?

☒ Inclusive Growth ☒ Health and Wellbeing ☒ Zero Carbon

9 Arrangements for the publication of decisions ensure that the Council is open and transparent in its consideration of the councils three Key Pillars.

Options, timescales and measuring success

What other options were considered?

10 The IDS Statement of Internal Control is a valuable source of assurance for the Committee and enables democratic oversight of arrangements. No other option was therefore considered.

How will success be measured?

11 Relevant performance indicators are set out in the IDS Statement of Internal Control.

What is the timetable for implementation?

12 The decision making framework is already in place and will remain so.

Appendices

13 A – IDS Statement of Internal Control

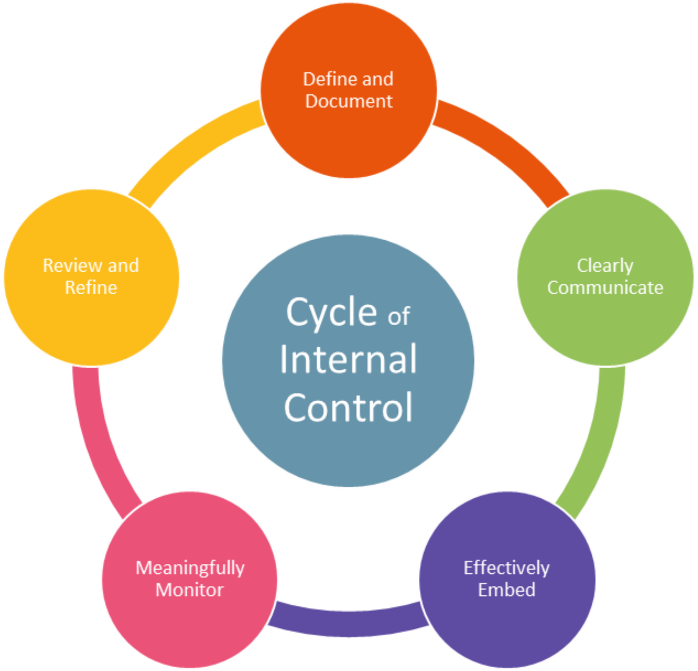
Background papers

14 None

This page is intentionally left blank

Introduction

1. This statement of internal control provides assurance in respect of the Council's internal control arrangements for the Integrated Digital Service; that they are up to date, fit for purpose, embedded, and routinely applied.
2. The arrangements are comprised of the documents, systems and processes which guide and control the way in which Integrated Digital Services are delivered to develop digital capacity and to support the strategic ambitions of the council.
3. In accordance with the principles and commitments set out in the Local Code of Corporate Governance, the arrangements seek to support the council in developing digital capacity and delivering services in line with the Council's values.
4. This statement sets out the arrangements for the internal control of Integrated Digital Services over the reporting period from March 2023 to February 2024.
5. The statement includes opportunities that have been identified to improve these arrangements.



Define and Document

1. **Policies and Strategies**.
2. The following policies and strategies are subject to change, pending the work being undertaken by the new Corporate Transformation team and new processes which may be introduced.
3. The policies and strategies which underpin the governance for the Integrated Digital Services are detailed in the following table.

• Digital strategies	• A set of digital principles have been defined which set the parameters for how Integrated Digital Services develop new technical solutions and ensure that architectural decisions align to these principles. An example being Cloud First[1] as a guiding principle. • Integrated Digital Services have recruited an Enterprise Architect who is developing and Enterprise Architecture strategy which will help the organisation to understand the business functions, IT, data, and risk perspectives and then effectively plan for success. • The Integrated Digital Services Solution Architects have been aligned to the Enterprise Architect to ensure they all follow the same architectural design pattern.
• Digital priorities	• Integrated Digital Services through the Digital Change function, work closely with directorates to plan their IT requirements, exploit Line of Business Products[2] and then, through the Digital Board, prioritisation is aligned to planned work across the council.
• Information Management & Governance (IM&G)	• Please see separate report on this agenda; the Annual Information Governance Report, including the Annual Report of the Caldicott Guardian.

[1] Cloud first is a strategy that prioritizes the use of cloud computing in an organization's IT infrastructure. This means that when considering new IT initiatives, the first option to be evaluated should be cloud-based solutions, rather than on-premises solutions. This approach can help organizations to reduce costs, improve scalability and flexibility, and take advantage of the latest technologies. The UK government has a "Cloud First" policy, which means that central government departments must consider and fully evaluate potential cloud solutions before considering any other option. 1

[2] Line of business (LOB) applications are software programs that are used the council to support its specific business operations and processes. These applications are typically designed to meet the unique needs and requirements of the Directorate or Service Area, and can include tools for managing customer relationships, financial transactions, inventory, and more. LOB applications can be custom-built in-house, purchased from a third-party vendor, or a combination of both. They can be deployed on-premises, in the cloud, or in a hybrid model.

4. **Roles and Responsibilities**.

Officer Roles and Responsibilities	
• Director of Strategy and Resources	• The Director of Strategy and Resources has overall responsibility for the Integrated Digital Services function and works closely with the Chief Digital Information Officer to set IT strategy and direction. The Director of Strategy and Resources is also the Senior Information Risk Owner for the Council.
• Chief Digital Information Officer (CDIO)	• The Chief Digital Information Officer has full accountability for the Integrated Digital Service within the council. All Digital Service decisions, including any financial spend on Digital products or services are the responsibility of the Chief Digital Information Officer. The Chief Digital Information Officer is responsible for setting Digital strategies and for the effective planning of future Essential Service Programme capital spend requirements. Chief Digital Information Officer acts as Deputy Senior Information Risk Owner when the Director of Strategy and Resources is not available.
• Chief Technical Officer	• Chief Technology Officer is responsible for leading the technical, innovation, and digital architecture strategies for the Council, Integrated Care Board, and city organizations. The Chief Technology Officer will ensure service delivery meets the required performance standards and the statutory duties of the authority. The Chief Technology Officer works as part of the senior leadership team, modelling values and behaviours to help achieve the ambition of becoming the best city council in the country.
• Digital Change	• The Digital Change team are responsible for ensuring directorates can leverage the maximum return from their investments in digital products and services. Through effective product management, the Digital Change team own the full lifecycle of products and ensure change, contract management, training, product performance optimum, and digital transformation. • The Digital Academy within Digital Change is responsible for ensuring Council staff and citizens are effectively trained and digitally included to enable them to drive maximum value from digital products and services.
• Service Managers	• Service Managers within Integrated Digital Services are responsible for ensuring their areas of responsibility are managed effectively and that planning is established to ensure effective management of the area.
Governance bodies – Integrated Digital Service	**Responsibility**

• Pre-Digital Board	• To review work requests to ensure they meet strategic direction and are in line with Digital Roadmaps[3] and the council's Financial Challenge requirements and other organisational priorities. • Approved work to progress: ○ as Business as Usual (BAU) ○ as part of an established programme (e.g. Essential Services Programme, website redevelopment) ○ New developments/opportunities for digitisation of processes and services. • to be presented at Digital Board for prioritisation
• Digital Board	• To set the strategic direction for the Digital Board, ensuring digital enablement is aligned to the City Vision and strategic outcomes, making Digital by Design[4] a reality. • To set the priorities and delivery order for work being done by Integrated Digital Services. • To build Digital Roadmaps, in partnership with our stakeholders that represent the future direction of the Region, City Health Partnership and the council. • To support the ethos that we make digital technology easier, cheaper and faster for citizens to deal with the council, and for staff to provide services to citizens. The way in which we deliver this principle is by linking the work of Integrated Digital Services to the needs of customers and delivering services that are high impact and value-adding. • There is a documented Terms of Reference for the Digital Board. • To approve all work requests for Integrated Digital Services effort. • Track and monitor progress of the Integrated Digital Services Portfolio dealing with any escalated issues. • Prioritise work requests.
• Procurement Approval Meeting	• To review contract renewals and procurements, ensuring that all options have been considered prior to awarding external contracts and ensuring Value for Money
• Resource Management Meeting	• To effectively plan Integrated Digital Services resourcing to ensure adequate staffing levels with the appropriate technical skills are in place in a timely manner. • To work with Service Managers to understand future required technical skills and then plan to have these in place within the service.

[3] A digital roadmap is a strategic plan that outlines how an organisation will use technology to achieve its goals and objectives. It provides a high-level overview of the digital initiatives and projects that will be undertaken, and the timeline for their implementation. A digital roadmap can help organisations to align their technology investments with their business strategy, prioritize their digital initiatives, and communicate their plans to stakeholders.

[4] Digital by design is a strategy that aims to deliver services and products in a digital-first manner. This means that digital solutions are prioritized and designed to be the primary way for users to interact with an organisation. The goal is to create user-friendly, efficient, and cost-effective digital services that meet the needs of users and improve their overall experience.

	• To assess whether offshoring or outsourcing of skills to augment the Integrated Digital Services team is appropriate.
• Design Authority	• The Design Authority is comprised of technical roles within Integrated Digital Services and meets weekly. Its function is to review technical papers to ensure design principles are followed and align to the technical roadmap. • The Design Authority is Chaired by the Chief Technical Officer. • There is a documented terms of reference for the Design Authority.
• Change Advisory Board (CAB)	• The Change Advisory Board run formal meetings to assess, prioritize, authorize, and schedule changes as part of the change control process. • The Change Advisory Board is chaired by the Head of Cloud & Platforms.
• IM & G	• Please see separate report on this agenda Annual Information Governance Report, including the Annual Report of the Caldicott Guardian
• Change Delivery Group	• Monitor delivery of the Integrated Digital Services Portfolio – specifically, budget, risks, issues, dependencies, benefits and resources. • Approve communications on Portfolio progress. • Make recommendations to the relevant forums on the termination of initiatives. • Agree the processes contained within the Portfolio Delivery Cycle and ensure that they work effectively. • Approve changes to the practices within the Portfolio Delivery Cycle. • Undertake periodic reviews of the effectiveness of Portfolio Delivery and take appropriate action where required.
Governance Bodies – Service	**Responsibility**
• Corporate Leadership Team	• The Corporate Leadership Team (CLT) are responsible for ensuring that Integrated Digital Services have robust and aligned service plans to ensure each directorates digital ambition can be delivered. CLT members attend Digital Board and use this as the forum to set the strategic direction for the council, ensuring digital enablement is aligned to the City Vision and strategic outcomes, making Digital by Design a reality.
• Integrated Digital Service – Senior Leadership Team	• The Integrated Digital Services Senior Leadership Team meet every week and have a set agenda which includes a monthly financial review, a review of service performance and a Cyber update.
• Programme & Project Boards	• Each major programme and project have their own Board to oversee delivery, manage risks, budget, quality, and timeframes.

• Strategic Investment Board	• Reviews capital funding requests from Directorates, prioritises and provides approval based on the merit of the request.
Democratic Oversight:	**Responsibility**
• Executive Member	• The Executive Board portfolio holder for Strategy & Resources aligned to Integrated Digital Services is regularly briefed by the CDIO on key decisions and the Digital Strategic direction. The Executive Member is responsible for ensuring Integrated Digital Services plans are scrutinised and approved prior to commencement of work.
• CGAC	• The Corporate Governance and Audit Committee is responsible for reviewing the adequacy of the council's governance arrangements, including Integrated Digital Services. The Committee receives an annual assurance report on Integrated Digital Services management arrangements from the Director of Strategy and Resources and uses this to monitor, review and scrutinise these arrangements and their implementation.

Clearly Communicate

5. Training and Guidance

Digital Inclusion:

- 100% Digital Leeds is one of the most successful, high-profile, and well-respected digital inclusion programmes in the country. The team leads digital inclusion for the city and our approach is recognised as best practice by the country's leading experts on digital inclusion. We feature as a case study in reports by The King's Fund, The British Academy, The Fabian Society, Local Government Association, NHS England and more. We were funded to create the Digital Inclusion Toolkit and publish our approach on there so that other councils could follow our lead.
- Digital inclusion/100% Digital Leeds are referenced in (and support the delivery of) numerous council strategies including the Best City Ambition, Better Lives Strategy, Living with Dementia in Leeds Strategy, Inclusive Growth Strategy, Future Talent Plan, Leeds Housing Strategy, Health and Wellbeing Strategy, and the Digital Strategy. We work at the organisational level rather than working directly with people/communities who are digitally excluded. Within the council we work with colleagues across Integrated Digital Services, Employment and Skills, Culture and Economy, Adults and Health, Children and Families, Communities, Housing and Environment, and more.
- In addition to working with council colleagues, we work at a strategic level with over 200 delivery partners including teams, services, settings, and organisations across the city and across sectors (council, third sector, digital and tech sector, health and care, academia).
- We strengthen the digital inclusion infrastructure across the city by bringing together organisations in a place or serving a particular community to address challenges at scale. We build digital inclusion capacity and confidence within organisations and across sectors, guiding and supporting partners at every stage of their development journey.
- We focus on priority neighbourhoods and communities most likely to experience (digital) exclusion, including ongoing work with organisations supporting older people, migrants and refugees, people with learning disabilities and autistic people, residents of care settings, women and families, people with long-term health conditions, people living in poverty or on a low income, and more.

- We've brought in over £1million funding every year for each of the last three years (£800,000 so far this financial year). Almost all of that funding has been used to increase the digital inclusion capacity of community organisations, supporting inclusive growth principles and increasing third sector resilience.
- **Priorities for 2024/25 include:** lead Digital Inclusion West Yorkshire, funded by WYCA with support from the Mayor of West Yorkshire to expand the 100% Digital Leeds model across the region; work with Leeds Digital Ball to raise funds from the digital and tech sector to support digital inclusion – and work with the organisations who receive the funding; work with digital and tech sector representatives and Leeds Community Foundation, Voluntary Action Leeds and Forum Central to support the priorities identified in the Community and Third Sector needs from Digital Transformation report; work with colleagues in Adults and Health to support the rollout of the Digital Social Care Record and other digital transformation projects across social care; work with Primary Care, Community Healthcare and colleagues across the NHS to support the adoption and effective use of digital health tools and technologies; support channel shift and realise efficiencies by working with colleagues in Integrated Digital Services and across the council (plus organisations across the city) to support the adoption of online services by digitally excluded people and communities who are currently the heaviest users of telephone/face-to-face council services.

Digital Learning:

- Disparate teams with different ways of working have come together as one Digital Learning team. We are defining our new ways of working across the Digital Learning team based on seven core behaviours, with an increased focus on outcomes as well as outputs.
- We continue to deliver ongoing digital skills training online of business applications across the council, aligned to Directorate/Service priorities and Integrated Digital Services Product Management roadmaps.
- We're developing new online and self-service learning offers for colleagues, alongside face-to-face support for colleagues who may struggle to access online training. We have embedded the digital learning resources into SharePoint and Teams to enable colleagues to more easily find the learning that's most relevant to their role.
- Working with User Researchers from the Digital Transformation team to review the M365 learning offer, including a new 'Champions' approach so that more colleagues can more effectively promote the benefits of digital and offer peer support.
- We're also working with external suppliers and partners to create higher-level training offers for digital skills in Integrated Digital Services and across the organisation. We will leverage contacts and contracts to make best use of digital skills support and resources from suppliers, providers, partners, and digital and tech companies to meet identified need more effectively and efficiently.
- We convene and co-chair with Employment and Skills a cross-sector digital skills network. Working with partners to take a whole city approach, identify and fill gaps, avoid duplication, and make best use of our collective resources and capacity. Includes representatives from Adult Education, Employment and Skills, Forum Central, Leeds City College, Leeds Health & Care Academy, Leeds Libraries, Leeds Teaching Hospitals Trust, Luminate Education Group, Strategy and Innovation, Thrive By Design.
- **Priorities for 2024/25 include:** Support the rollout of Core Business Transformation, especially for colleagues who are currently 'offline' from a council perspective; develop a Digital focus for the Be Your Best programme; support the rollout and adoption of Microsoft Co-Pilot to ensure the technology can deliver efficiencies through new ways of working; lead by example, influence culture change at all levels, build digital leadership, confidence and resilience across the organisation.

Across both areas of 100% Digital Leeds, strategic priorities include:

- Continue to bring in external funding to address the financial challenges and capacity pressures faced by the council, third sector, and health and care.
- Ensure services and interventions are more joined-up, efficient and effective rather than fragmented offers.

- Achieve shared priorities and outcomes more efficiently and effectively through closer working across sectors.
- Create clearer pathways so that everyone can find the right help, delivered in the right way, by the right people, in the right place, at the right time for them.
- Ensure the digital learning and digital inclusion infrastructure continues to grow and evolve to meet people's changing needs as their lives, careers and circumstances change.

In summary, increasing digital inclusion and digital skills are enablers to achieving other priorities. When they lead to individual behaviour change, the resource savings and benefits are realised for everyone. Individuals can save time and money, services can be more efficient and effective, organisations can support people in ways that are more meaningful and holistic. Digital inclusion and digital skills are enablers to help people achieve their personal and professional goals, and services achieve their strategic priorities and outcomes.

6. Leadership

The leadership team and extended Service Leadership Team meet weekly and, when relevant, discuss internal controls. This group reviews the effectiveness of existing controls and discuss improvements if required.

The weekly Service Leadership Team meeting is structured to ensure monthly updates are provided on finance, sourcing, Cyber, Service Desk Service Level Agreement performance, updates from the CDIO from Strategy and Resources, Service Leadership Team and the Integrated Care Board Executive Management Team meetings.

Following the full Service Leadership Team meeting there is an Extended Service Leadership Team meeting. This meeting is for the next tier of management within Integrated Digital Services and is focused on debriefing the group on Service Leadership Team and then focussing in on a specific subject, led by a member of Extended Service Leadership Team.

There is a weekly Service Leadership Team catch up every Monday morning, which is focussed on the week ahead and allows the Chief Digital Information Officer to task Service Leadership Team members with specific actions or priorities for the week ahead.

Effectively Embed

Establish Expectation
Facilitate Compliance
Observe Outcomes

Establish Expectation: Establish arrangements that are proportionate, practicable and compliant

7. Directorate Digital Road maps

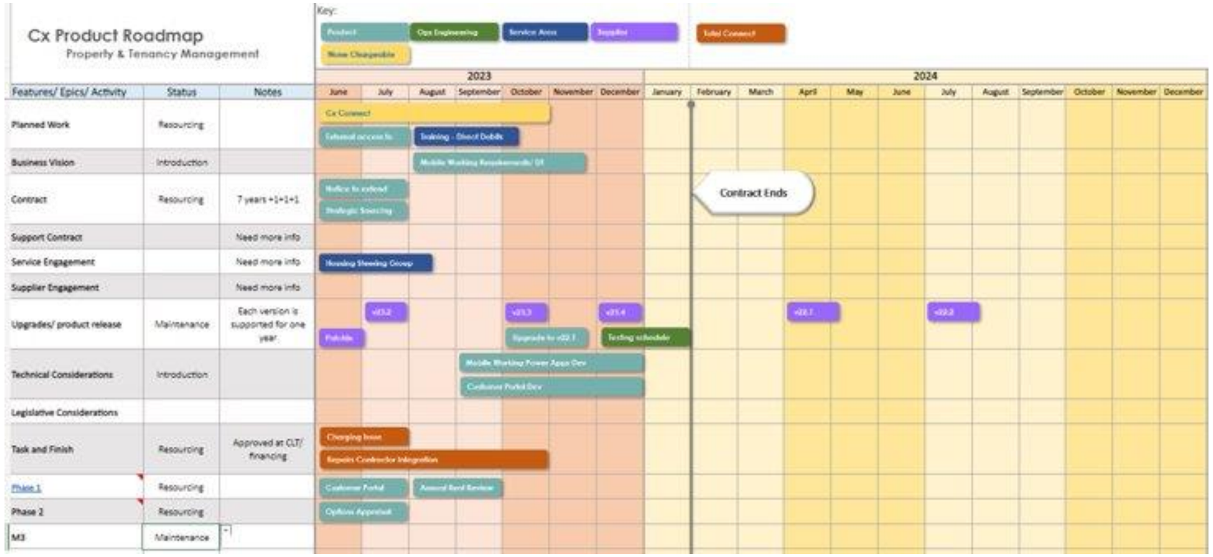
Definition:
*A **Product Roadmap** is a visual summary that maps out the vision and direction of a product.*

They contain the following information:

- Contract review, and end dates plus, contract extensions if available
- Supplier product release dates
- Release upgrades to be implemented.
- Planned work – new modules, system configuration, business process reengineering, functionality augmentation through automation
- Business vision / requirements – mobile working, process automation
- Technical strategy / roadmap (when available, currently under development)

Product roadmaps exist for the majority of the products, and the remainder are in production.

Example of a product roadmap:



Cx Product Roadmap
Property & Tenancy Management

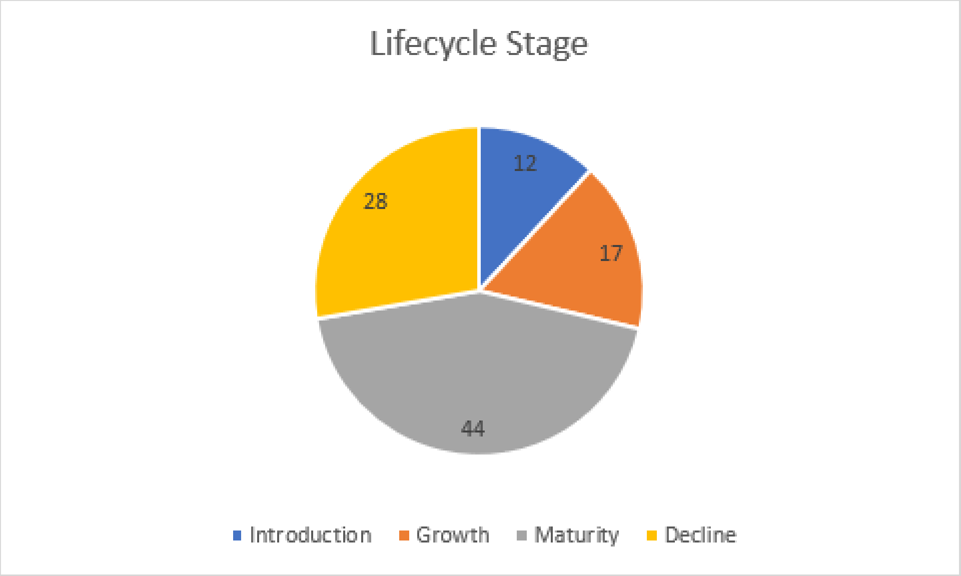
Features/ Epics/ Activity	Status	Notes
Planned Work	Resourcing	
Business Vision	Introduction	
Contract	Resourcing	7 years +1+1+1
Support Contract		Need more info
Service Engagement		Need more info
Supplier Engagement		Need more info
Upgrades/ product release	Maintenance	Each version is supported for one year
Technical Considerations	Introduction	
Legislative Considerations		
Task and Finish	Resourcing	Approved at CLT/ financing
Phase 1	Resourcing	
Phase 2	Resourcing	
M3	Maintenance	

Product data:

- A Master repository has been created to pull together data from various repositories for all Integrated Digital Services portfolio items (repositories: Technical Services Portal, LCC Applications List Product Data Sheets, Contracts Work Tracker)
- Data includes: hosting, number of users, lifecycle stage, stakeholder information
- Data collection, and cleansing from multiple repositories is continuing to form a trusted “Single Version of the Truth”.

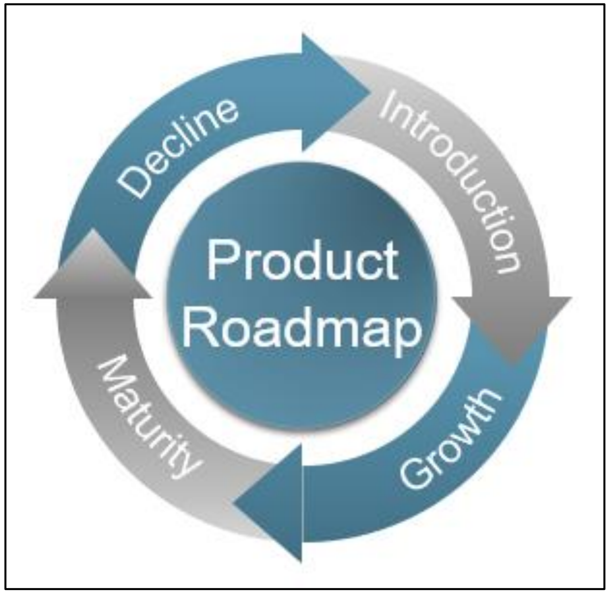
Integrated Digital Services Product Portfolio :

- 101 managed products (which includes contract management, implementing upgrades, training, support, etc.):

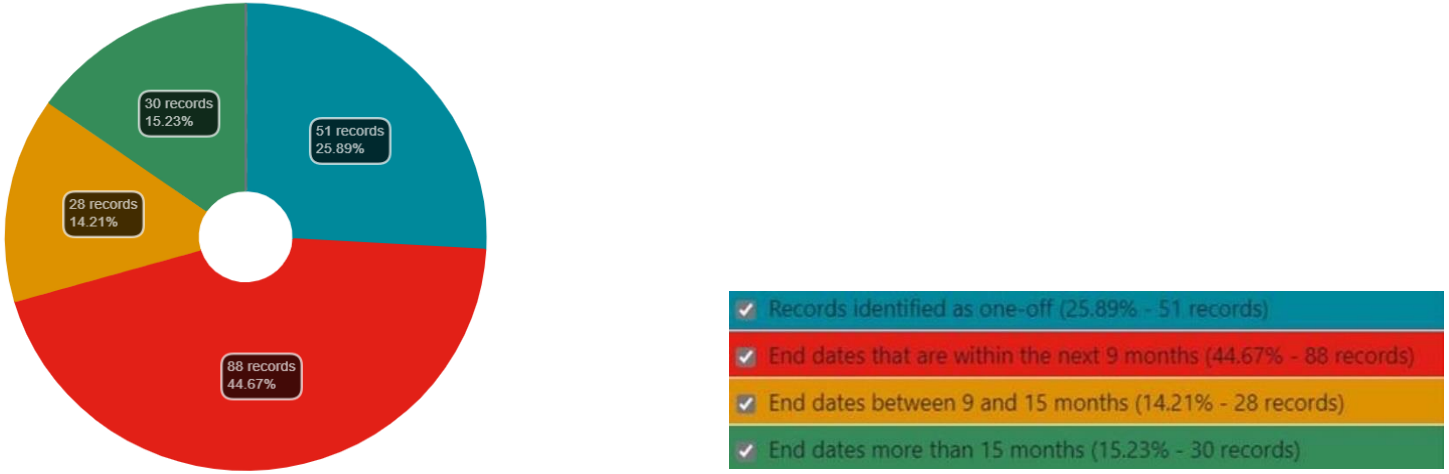


Introduction (Implementation): New product in the process of being implemented.
Growth (Improve): Product in live usage with improvements continuing.
Maturity (Maintain): Stable product with no major development work being implemented.
Decline (Decommission): Decision made to replace or decommission.

Diagram - Product Life Cycle



There are currently 197 contracts that are in product management (negotiating renewals, ceasing contracts):



- NB, of the approx. 600 items on the wider Integrated Digital Services portfolio, 298 currently sit within Product Management with the remaining items being software licences, access databases, local installs, and technical / infrastructure applications.

Next Steps:
Product management have engaged with UST Global[5] for a four-week period, and have recommendations on the production of product roadmaps, which will be implemented once a solution has been procured.

The intention is for Lean IX[6] to replace ProductPlan[7] (we only have a static view of ProductPlan, as the contract was not renewed, and is in the process of being decommissioned) allowing the data, and roadmaps to be linked together to create high level Service Roadmaps.

The technical road maps for Integrated Digital Services infrastructure and enterprise architecture requirement development in the coming months, which will then allow dependencies to be considered alongside future product development, and decision making.

Until we have a dynamic tool such as Lean IX, our current estate of Product Road Maps, will remain one dimensional.

8. Integrated Digital Services Identified work streams.

Integrated Digital Services workstream mainly consists of the following -

- Business as usual - any work where everything is proceeding as normal and as expected.
- Portfolio of change - Programmes and Projects delivering technical / digital and or business changes across the council.
- Integrated Digital Services has the following major funding schemes:

Essential Services Programme (ESP) – This Programme delivers a range of major essential IT infrastructure and application initiatives covering technology investments, refresh of ageing devices, upgrades of systems and the ongoing protection of data and information.

At a Strategy and Resources level the ESP Programme contributes to the following strategic objective:

- Improving our digital offer by enhancing digital skills, automating manual processes where possible, providing more technology services and infrastructure via the internet (cloud-based), and giving all staff, including those on the frontline greater access to digital tools and technology.

[5] UST Global is a multinational provider of digital technology and transformation, IT services and solutions. They have been award contracts with the Integrated Digital Service to provide support for various digital projects.

[6] Lean IX is LeanIX is an enterprise architecture software that provides a platform for companies to manage their IT architecture and drive their digital transformation. It allows organizations to visualize, plan, and manage their IT landscape, including applications, technologies, and processes.

[7] ProductPlan is used to build strategic roadmaps, align behind customer needs, prioritse, and measure success.

To support the strategic objective and the programme outcomes and benefits the following key objectives will be delivered:

- To refresh end of life LCC security infrastructure and engineer in continued improvements covering areas such as, firewall protection, anti-virus, file storage scanning, secure transfer of files, web and content filtering. This is a key objective of this programme to ensure Integrated Digital Services maintains a strong security posture providing the ability to identify, respond to and recover from security threats and risks.

- To move away from on-premise storage to a Cloud based service offering enhanced data security, redundancy (archive / backup), supporting greater collaboration on documents and files, scalability (on demand) and in lock step with current and evolving legislative and data storage compliance.

- To replace and refresh existing information governance systems and processes to support data classification, data cleansing, data retention and data destruction to ensure robust data protection and maximise cost savings through IG management and control and through optimal use of storage media (storage tiers).

- To undertake a health check and complete remedial actions to ensure continued Public Services Network (PSN) compliance. This will involve specialist external support to identify vulnerabilities across the network infrastructure and systems and agreement on what additional measures are needed to meet the stated security standard.

- To undertake an audit of the current Payment Card Industry (PCI) security standards to ensure that all card payments processed within LCC are and remain fully compliant.

- To ensure the continued availability and security of existing digital devices (laptops, tablets, smartphones) issued to LCC staff through the provision of timely and cost-effective break / fix service, thereby extending the life of these assets to maximise the return on investment.

- To invest and expand latest wi-fi provision to agreed locations forming part of the programme scope.

- To modernise and reduce the number of Multi-Functional Devices print (MFD) devices which will support greater sustainability (less energy usage) and reduced operating costs.

- To implement changes in a cost-effective way coordinating cross project activities where possible – for example fitting of replacement data centre generator at the same time of fitting new Computer Room Air Con (CRAC) units.

- To ensure existing Disaster Recovery (DR) and Business Continuity Plans (BCP) are fully assessed for impact and updating to ensure these remain robust.

- To ensure an optimised license model across all infrastructure and software components.

- To implement changes where possible reducing the need for downtime.

Digital Efficiencies Programme (DEP) – This Programme focused on delivering digital efficiencies across the council. The DEP Board is responsible for reviewing, approving, or rejecting changes to the programme, including additional budget allocation, requests for additional resources, and changes to the scope of existing projects.

DEP Programme Objectives – 2024/25

The Digital Efficiencies Programme (DEP) focuses on innovating, improving, and transforming ways of working and how services are delivered.

It is recognised that the needs of our customers and how we can deliver services has changed a lot in recent years. The programme's focus is on becoming a customer-centric, digital first council that makes the best use of our resources and technology, to improve service delivery and drive savings over the next 3 to 5 years.

DEP contributes to the following strategic objectives:

- Improving our digital offer - enhancing digital skills, automating manual processes where possible, providing technology that enable self-service digital channels and AI and giving all staff, including those on the frontline, greater access to digital tools and technology.

- Improving efficiency - by reducing unnecessary admin overheads via modern technologies and processes which support a more streamlined function, reducing complexity and using standardised, reusable patterns. Adopting new technology and ways of working that reduce costs and increase the organisation’s effectiveness.

- Improving Customer Services - designing our services to meet customer needs (not the technology) and using quality information and data to support decision-making and how our services are designed. We will enable people to take full advantage of modern technology to ensure that our services are convenient, efficient, valued and easy to use.

To support the council's Best City strategic objective the programme will aim to deliver the following key objectives:

- Improve customer experience by delivering services that meet or exceed customer expectations.
- Empower customers to access and manage services online, anytime, anywhere, through easy-to-use self-service capabilities.

- Reduce the cost and complexity of service delivery by streamlining processes, eliminating duplication, and leveraging digital platforms.
- Improve our services by listening to customer feedback and using this to design our services.

Cloud Applications & Compliance Programme (CACP) - This Programme ensures the LCC Application estate is compliant by meeting statutory and regulatory requirements and where possible is reducing the overall cost to the Council via application rationalisation and innovation, and the delivery of business outcomes via more efficient technical solutions.

At a Strategy and Resources level the Cloud, Applications and Compliance Programme contributes to the following objectives:

- Improving our digital offer by enhancing digital skills, automating manual processes where possible, providing more technology services and infrastructure via the internet (cloud-based), and giving all staff, including those on the frontline greater access to digital tools and technology.
- Improving efficiency of how we do business as a council by reducing unnecessary admin and support overheads via modern technologies and processes which support a more streamlined function.

To support the strategic objective and the programme outcomes and benefits the following key objectives will be delivered:

To maintain our compliance with key legislation and security measures, including PSN, PCI-DSS and GDPR, by ensuring our applications can record an audit trail, are protected by our infrastructure, protects customer information, supports data cleansing, data retention and data destruction and any end-of-life applications are replaced with modern, secure, and compliant technologies. This is a key objective of this programme and CACP will work closely with ESP to ensure both application and infrastructure compliance are covered.

To move away from on-premise storage to a Cloud based service and taking the opportunity to rationalise the LCC application estate, by refactoring, re-platforming, repurchasing, rehosting, relocating, retaining, or retiring applications. A Cloud based service will offer enhanced data security, support greater collaboration, and allow LCC to keep up to date with ever evolving legislation and data storage requirements.

To implement an Integration platform using Azure Integration Services (AIS) and replace services hosted on the existing BizTalk and GlobalScape platforms. This will help towards our goal of modernising the LCC estate, as well as improving efficiencies within the integration team by combining skill sets."

Facilitate Compliance: Ensure appropriate tools and sufficient resource to enable compliance

9. Daptiv – this is the tool used by the Integrated Digital Services Portfolio Management Office (PMO) to plan and track delivery of all work being undertaken across Integrated Digital Services. It manages all Integrated Digital Services resources and is used to understand capacity, availability and demand management. Timesheets are completed by all staff in Integrated Digital Services via Daptiv and these are used to ensure appropriate recharging is undertaken to the relevant capital scheme or revenue budget. Timesheet analysis is also used to help determine capacity issues.

Significant work has been undertaken in the last quarter on improving forecasting and resource scheduling to better understand demand. The tool is also used to track and report on progress, issues, risks, dependencies, budgets and benefits.

10. There are various Funding streams within Integrated Digital Services, overall operational budget for staffing, Essential Service Programme, Cloud Applications & Compliance Programme and the Digital Efficiencies Programme. These are all capital programmes which are reviewed each year.

11. Where additional funding is required for the Essential Service Programme, Cloud Applications & Compliance Programme and the Digital Efficiencies Programme capital programmes, Integrated Digital Services will bid via the Strategic Investment Board for funding. The Strategic Investment Board overseas capital funding requests from Directorates and assesses their merit against other requests that have been presented before approval.

12. The Essential Service Programme, Cloud Applications & Compliance Programme and the Digital Efficiencies Programme capital programmes of work are reported to Digital Board and a governance board comprised of representatives from Integrated Digital Services and Internal Audit has been established to oversee the schemes.

13. Spend on Essential Service Programme, Cloud Applications & Compliance Programme and the Digital Efficiencies Programme is closely monitored and reviewed. During 2023/24 it was recognised that the financial challenge affecting the authority required even closer scrutiny on spend on these programmes. After reviewing them, a decision was taken to hand back £1m capital which had previously been identified for device refresh but was no longer required/essential. This decision was discussed and agreed at Integrated Digital Services Senior Leadership Team.

14. A review of the Essential Service Programme scheme for 2024/25 has been completed with many schemes moved back a year to 2025/26in order to reduce spend in the current year. Additionally, a decision has been taken to pause rollout of Windows 11 due to Microsoft putting Windows 10 into extended support. This means a projected Integrated Digital Services spend of £2.9m on devices in 2024/25 has been reduced to a spend of £1m. The focus instead will be on replacing break/fix devices with new devices, which will be imaged to Windows 11. This will allow a slower deployment of Windows 11 without the need to perform a full estate refresh. The Windows 10 rollout took two years to complete at a cost of approximately £1m in project and resource costs.

15. Risks – Integrated Digital Services has responsibility for managing three risks on the council's corporate risk register: Major IT failure, Major cyber-incident and Information Management and Governance. Additionally, Integrated Digital Services are involved with managing digital and technology risks on council programmes and projects and providing periodic health checks and RAG (Red Amber Green) status updates for them. The health checks consider the IT risks, issues, budget, scope, resources, and schedule.

16. An Internal Audit review of Cyber Security Risk Management was undertaken during 2023 to review the controls in place to manage cyber risk. This resulted in a report bring produced (October 2023), in which several recommendations have been made, the Integrated Digital Services are working on with colleagues in Intelligence and Policy. Work is progressing on the recommendations with a timescale to complete during 2024. Progress against these recommendations is monitored by Internal Audits recommendation tracker.

17. The objectives of the audit and their recommendations are:

Objective 1: To ensure the LCC Risk of Major Cyber Incidents is appropriately recorded, continually updated, managed, and reported on. In doing this the Major ICT Incident risk will also be looked at to identify appropriate cross over in risk and mitigating controls listed.

Objective 2: To review the mitigating controls listed against this risk to assess whether: The controls listed are up to date and in operation; The mitigating controls listed are deemed sufficient to manage the risk per the risk appetite and to identify what other assurances are in place covering this area, e.g., PSN and other external accreditations or assessments.

Objective 3: To ensure there is a major incident process in place. This will include looking at whether prioritisation over the order in which systems will be recovered have been agreed.

Objective 4: To ensure there is appropriate Communication, training and guidance is issued to staff relating to the cyber threat and their responsibility in guarding against it.

Key Recommendation

The way in which Integrated Digital Services and the business interact and communicate should be reviewed to ensure all parties are properly engaged and working towards the same goals. The Major Cyber Incident risk should be reviewed and re-written in a more user-friendly way that focuses on the key potential consequences to the council as a whole and the key services provided. Getting key staff from the wider business involved in this could be a good way of promoting this to help ensure all parties are properly engaged and working towards the same goals.

The review of the major cyber incident risk should include consideration of the following:

• The risk appetite for this area bearing in mind it would be impossible to guard against all potential threats and threat actors.

• The risk should be written in a way that it can be understood by key staff from all directorates. The Annual Corporate Risk Management Report is written in such a way, although it is appreciated that the document would need to be longer, include more information, and list specific potential sources and controls, which in some instances could be technical in nature.

• Integrated Digital Services should lead on identifying the potential sources that could lead to a major cyber incident. They should then work with key staff from directorates to identify the potential consequences to the council. This would require input from all areas of the council.

• The existing controls should only list current controls that are in place. If an accreditation is listed as a control, it should be accompanied by a high-level description of what it is and what it covers.

• The wider business and Integrated Digital Services should then agree the appropriate mitigating controls to manage the risk, prioritisation of systems and data for
recovery etc., in the event of a major cyber incident.

• The risk should include an indication of the timescales it could take to recover systems from a major cyber incident. Whilst this would not be easy to estimate and would depend on the type of attack, the wider business must have an idea to allow them to have appropriate business continuity plans in place. Reference to attacks other councils have suffered previously and the time it took them to recover could help enforce this point.

• The risk should be monitored on a quarterly basis by a body that includes representatives from all areas of the council including Integrated Digital Services. This process should then help the business understand this risk and its potential effects on their services better and help Integrated Digital Services understand the business priorities and risks. This could be further reenforced by the introduction of regular communications to all managers and staff informing them of emerging and current threats, what needs to be done to mitigate them and any relevant guidance or training available on this area. It is understood that the provision of separate cyber security training is being considered. Introducing this would further raise the profile of this risk and the fact it is everybody's business and not just Integrated Digital Services. The recommended regular communications could be the Cyber Sentinel monthly newsletter produced originally for CLS but just widening its circulation.

The implementation of these recommendations should help ensure both Integrated Digital Services and the wider council are aware of this risk and its potential implications; it is correctly recorded in an appropriate format and allow better business continuity planning within service areas.

18. Procurement – Corporate Procurement Rules (CPRs) are followed when undertaking the procurement of services and solutions.

The sourcing team manages attends SLT monthly and provides reporting on contract expiry to allow SLT to set direction for each contract. This demonstrates forward planning to ensure compliance.

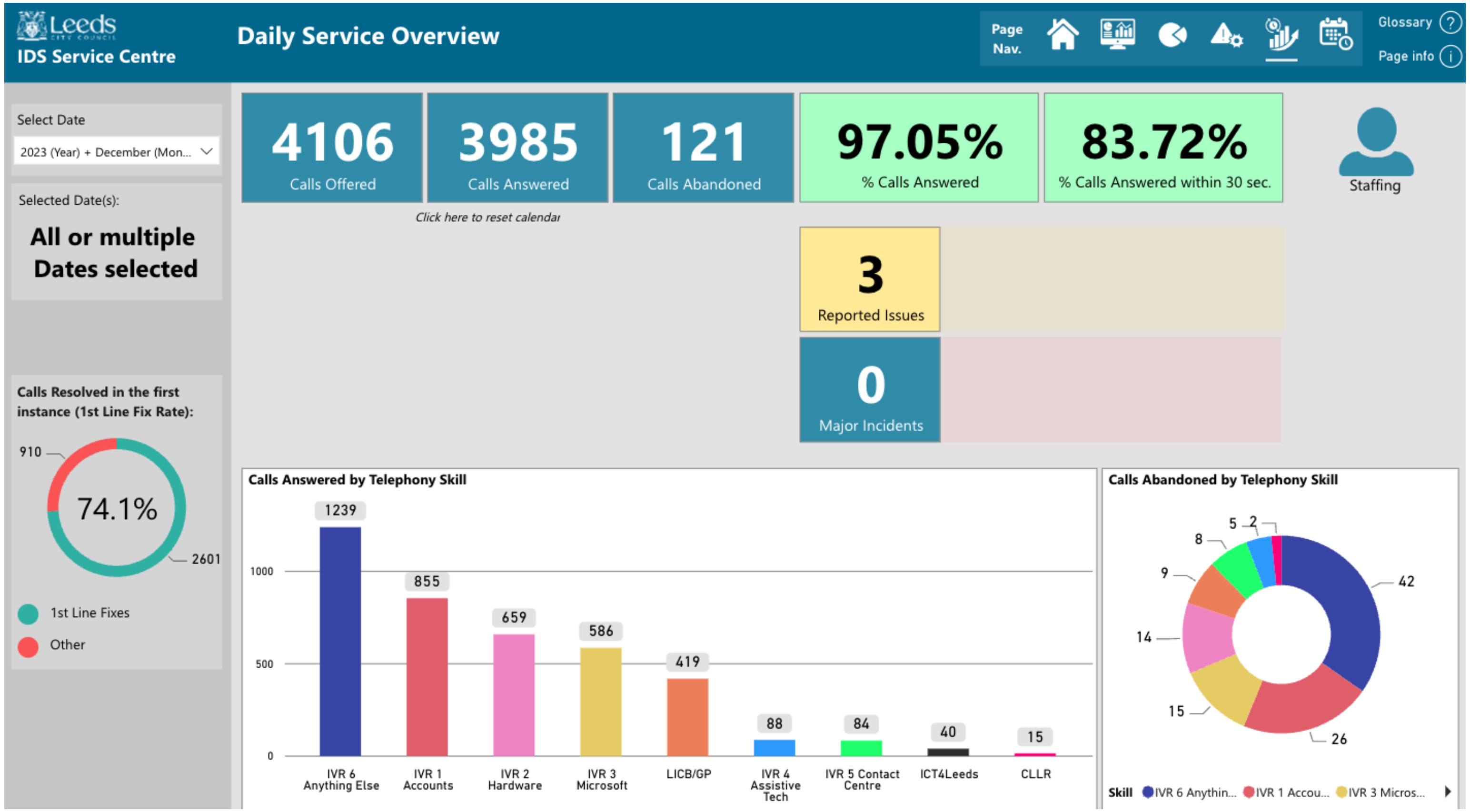
Observe Outcomes: Provide ongoing assurance that practice and procedure reflect expectation.

19. Daptiv reporting is used to provide assurance on delivery of all work across Integrated Digital Services.

Meaningfully Monitor

20. The Integrated Digital Services Service Centre produces monthly performance reports for a range of indicators. Performance is reviewed by Integrated Digital Services Senior Leadership Team. The main performance targets are to answer 70% of calls within 30 seconds, answer 93% of all calls offered, resolve 70% of calls at first line. If the reporting demonstrates poor performance against the indicators, such as long wait times on call for customers to get through to a Service Desk Agent, Integrated Digital Services Senior Leadership Team instigate a service improvement plan to ensure the desired targets are met.

21. The Integrated Digital Services Service Centre have produced a Power BI dashboard to provide reporting on performance against SLA. The image below shows call performance for 2023. The performance against all three SLA's exceeds the targets and reflect on the continued investment in this key area for Integrated Digital Services.



Leeds City Council
IDS Service Centre

Daily Service Overview

Page Nav.

Glossary ?
Page info i

Select Date
2023 (Year) + December (Mon...

Selected Date(s):
All or multiple Dates selected

4106	3985	121	97.05%	83.72%
Calls Offered	Calls Answered	Calls Abandoned	% Calls Answered	% Calls Answered within 30 sec.

Staffing

Click here to reset calendar

3
Reported Issues

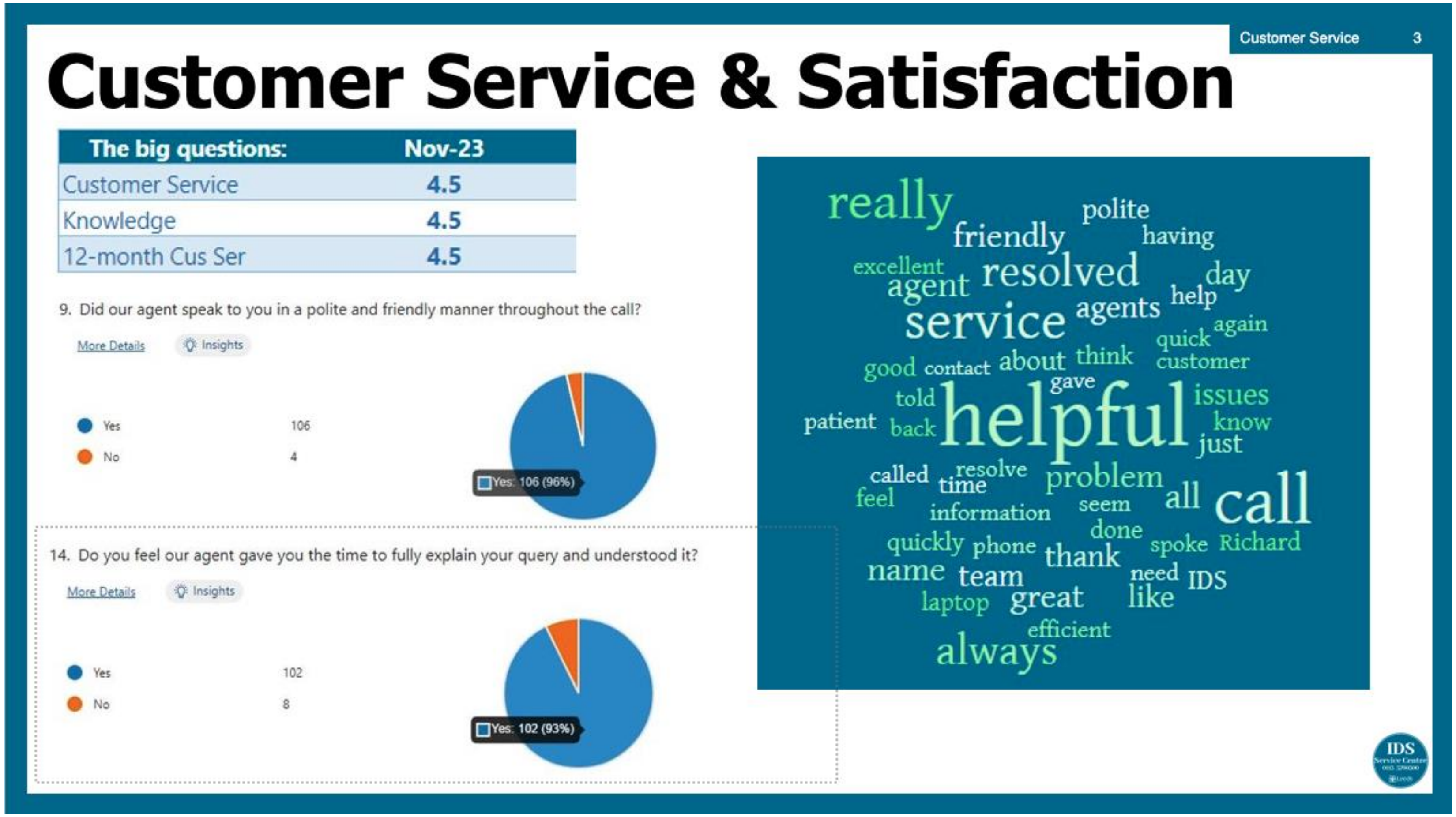
0
Major Incidents

Calls Resolved in the first instance (1st Line Fix Rate):

Calls Answered by Telephony Skill

Calls Abandoned by Telephony Skill

22. The Integrated Digital Services Service Desk recently completed a Customer Service and Satisfaction survey on calls. The image below shows that the team score 4.5 out of 5 for Customer Service, Knowledge, it also shows an average score of 4.5 for the previous 12 months. The word cloud captures the variety of regularly used words as feedback on the experience of contacting the Integrated Digital Services Service Desk.



Customer Service 3

Customer Service & Satisfaction

The big questions:	Nov-23
Customer Service	4.5
Knowledge	4.5
12-month Cus Ser	4.5

9. Did our agent speak to you in a polite and friendly manner throughout the call?

More Details Insights

● Yes	106
● No	4

14. Do you feel our agent gave you the time to fully explain your query and understood it?

More Details Insights

● Yes	102
● No	8

23. A report is produced Quarterly titled LCC 15 - ICT Major Systems Failure which is reviewed at SLT and CLT. This report focusses on two risks; Ensure ICT resources are effectively managed by SLT, Improve Forecast of Resource Planning. It is used to track Integrated Digital Services performance against both risks.

24. The ISaAC[8] Board monitors the degree to which LCC complies with its own security policies, current national standards for compliance and best practice using statistics and descriptive narrative generated by Operational Services' Service Centre (to guide current and future development work). It also produces the Public Services Network work programme to ensure the work required to successfully achieve the Public Services Network Code of Connection is complete in time.

Cyber Assurance and Security

25. The 2022 Public Services Network Code of Connection was submitted 27th September 2022 and a new Public Services Network Connection Compliance certificate was issued 14th October 2022.

26. CVSS stands for Common Vulnerability Scoring System and is a way for cyber security professionals to track the vulnerability level of different findings in a simple and easy-to-understand way.

27. For the 2023 Public Services Network Code of Connection accreditation a more stringent Common Vulnerability Scoring System (CVSS) has been introduced. The Cabinet Office now requires organisations to target CVSS v3 vulnerabilities. This has increased the number of CVSS 7 to 10 scores in this year's report from **131 to 264**.

28. The CVSS scores are rated as follows: Low: 0.1-3.9. Medium: 4.0-6.9. High: 7.0-8.9. Critical: 9.0-10.0

29. The average base score increased from 6.5 in CVSSv2 to 7.4 in CVSSv3. This means that the average vulnerability increased in qualitative severity from "Medium" to "High." As such the 2023 Public Services Network submission has been a much more significant programme of work and requires a greater degree of scrutiny to achieve certification.

30. Non-compliance with Public Services Network standards could leave the Council vulnerable to the following risks:
    a. The Head of the Public Services Network could inform the Department of Works and Pensions of our non-compliance. Continued non-compliance could culminate in denial of access to Revenues and Benefits data.
    b. The Head of Public Services Network could inform the ICO, which could culminate in the revisiting of the audit conducted by the ICO in 2013 to ensure compliance against the Data Protection Act / GDPR.
    c. The Head of Public Services Network could inform the Deputy National Security advisor to the Prime Minister, who would in turn conduct an assessment based on the national risk profile.
    d. The Head of Public Services Network could instigate an external audit of all our security systems by the National Cyber Security Centre. The Council could end up under partial commissioner control.
    e. Ultimately, the Head of Public Services Network could instigate a complete 'switch off' from Public Services Network services.

[8] The ISAac Board is a group that meets monthly to discuss cyber security and information governance issues in the Leeds City Council. The board members include representatives from different teams and areas such as the cyber team, the service centre, the integrated services, the cloud infrastructure, the security team, and the IG team. The board also reports to the Information Management Board and the Senior Leadership Team on the progress and challenges of cyber security and information governance.

31. Public Services Network certification is relied upon as an assurance mechanism to support information sharing, where many of the requirements request that the council present a certificate prior to sharing, or evidence alternative, more time consuming, compliance work to be completed.

32. Without a Public Services Network certificate, there is significant risk to the council's National reputation as a Digital Innovator.

33. The Public Services Network certificate was issued by Cabinet Office to Leeds City Council on the 23rd January 2024 with an expiry date of 23rd January 2025.

34. In terms of the monitoring of the Integrated Digital Services Portfolio, the PMO has established an independent Assurance function that will monitor and report on the status of major programmes and projects. Reporting will be into Integrated Digital Services, the relevant programme / project board, and the Digital Board.

35. Daptiv is also used to track and monitor all projects regardless of size. Each month the overall "Health" of projects is reported on and assessed by Integrated Digital Services Senior Leadership Team. This is a RAG status with Green being everything is on plan, Amber meaning attention is required and Red as a project is in trouble. The health categories reported on include Budget, Quality, Resource, Risk, Schedule, Scope and Benefits.

36. Following the 2022 Local Election project Integrated Digital Services received some criticisms from the Election team on Integrated Digital Service's handling of both the project and the actual count process. Following receipt of this feedback Integrated Digital Services met with the Elections team and put in place a service improvement plan. This SIP looked at all aspects of how Integrated Digital Services handled the project, including staffing, devices, application support, communications. Following this review new processes were introduced for the 2023 Election project, which resulted in a very positive process and excellent feedback received from the Elections team and Chief Executive. Given we are moving into a General Election in 2024, this puts Integrated Digital Services in as strong position to deliver a successful project.

37. The Children's & Families directorate raised concerns in early 2023 that Social Worker requests for new mobile phones were not being prioritised and resulted in delayed deliveries to customers. Integrated Digital Services recognised that there was a process failure and introduced a change to the MyIT form for requesting devices for Social Workers. A new field was added to allow the requestor to signify the device was for a Social Worker, this in turn allowed the Integrated Digital Services Sales team to be able to search on this field and prioritise these requests.

38. Throughout the year Integrated Digital Services have been developing skills in the Microsoft Power Platform, which has led to the in-house development of Power Apps for use by council employees.

39. The following PowerApps have been developed and are in use across the services listed.

App	Service
Legal Court Papers	Legal Services
Confidential Wast	Cleaning Services
Blocked Chutes	Cleaning Services
Mileage	Social Work (Corporate)
Incidents and Accidents	HR
Vehicle Checks	Highways
Out of Hours App	Contact Centre Out od hours team
Transport Booking App	Passenger Transport/Childrens
Cleaning Services DRIVER INFORMATION	Cleaning Service (CEL)
Fleet ACCESS TO SHARE POINT	Fleet (CEL)
Stage 2 Fire Safety Checks	Housing and Project Team
Door Checks	House
Pool Density	Active Leeds

40. The following PowerApps are in development and will be deployed in the coming weeks.

Current Priorities		
App	**Service**	**Status**
Job Sheets	Presto Clean	In Sprint
Home Care	Adult Social Care	In Sprint
Fleet Hire Vehicle App	Fleet (CEL)	Sprint Prep underway
Special Diets	Catering	In discovery - nearly sprint ready

Review and Refine

Adequacy and Resilience of Internal Controls

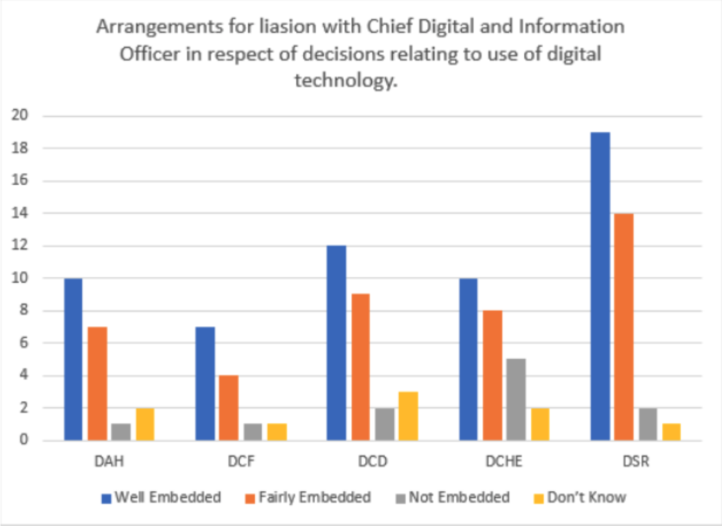
41. Several existing controls are still being imbedded as they link to the new organisational model for Integrated Digital Services. The service will continue to review and ensure that these are fit for purpose on an ongoing basis.

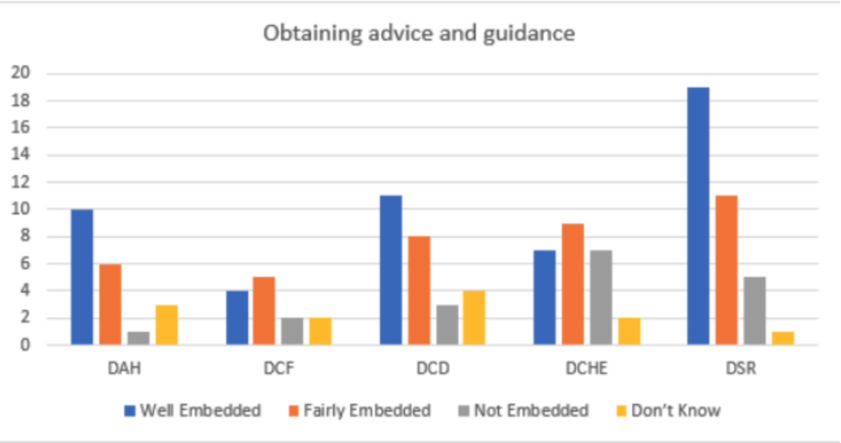
Survey of Internal Control

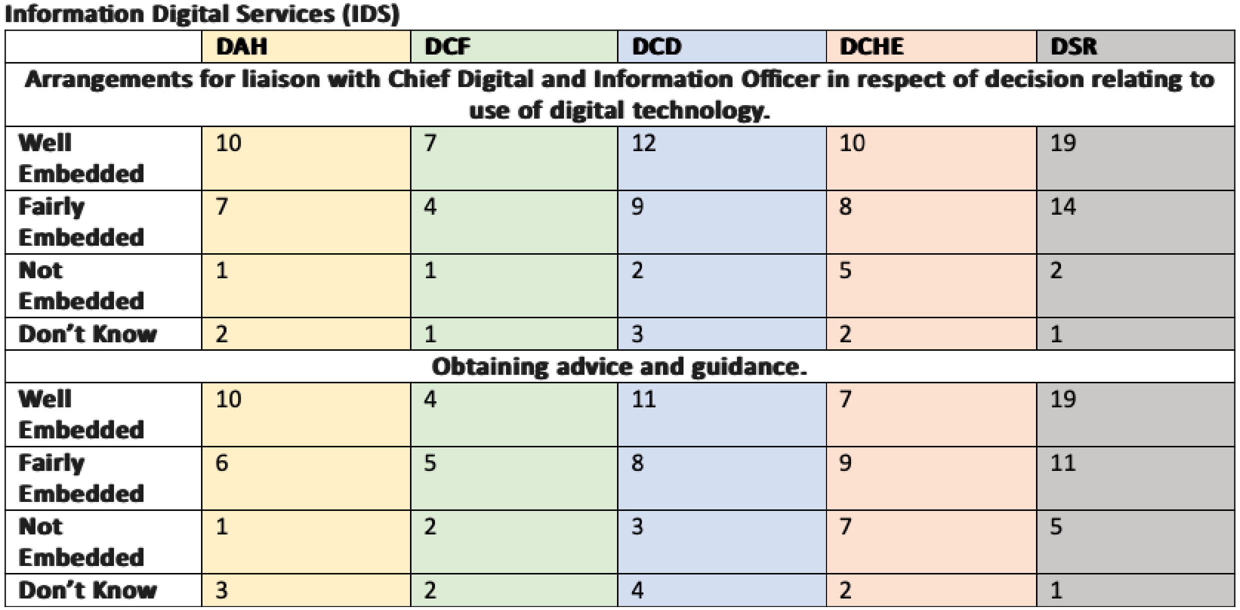
42. The survey of internal control asked operational managers to rate how well the council’s internal control arrangements are embedded.

43. The survey included the following questions about arrangements for governance of Integrated Digital Services including.

- obtaining advice and guidance, and
- arrangements for liaison with Chief Digital and Information Officer in respect of decisions relating to use of digital technology.







Information Digital Services (IDS)

	DAH	DCF	DCD	DCHE	DSR
Arrangements for liaison with Chief Digital and Information Officer in respect of decision relating to use of digital technology.					
Well Embedded	10	7	12	10	19
Fairly Embedded	7	4	9	8	14
Not Embedded	1	1	2	5	2
Don't Know	2	1	3	2	1
Obtaining advice and guidance.					
Well Embedded	10	4	11	7	19
Fairly Embedded	6	5	8	9	11
Not Embedded	1	2	3	7	5
Don't Know	3	2	4	2	1

44. The results show that decision making related to use of digital technology is generally understood across directorates, however there is clearly work to do in the Children's & Families directorate where five respondents state arrangements are not embedded.

45. Comparisons to previous years surveys are problematic given that the two questions asked in 2022 were different, they were; Arrangements for governance of Integrated Digital Services and Arrangements for sharing and cascading information.

46. Regarding the question asking about obtaining advice and guidance, again the response is generally positive. Children's & Families provide a similar response to the previous question with seven respondents stating arrangements are not embedded.

47. Integrated Digital Services Digital Change will discuss these responses with Children's & Families to understand the concerns and put in place measures to resolve.

48. Within the Survey of Internal Control there were two specific comments related to Integrated Digital Services:

Principle 4: Determining Effective Interventions.

a. There is not a lot of use made of the procurement framework, so it's one of these things where it's "relearnt". In terms of "We will ensure that decision makers are provided with relevant, timely information to support decisions which are proportionate, sustainable and realistic to meet identified aims and outcomes" we have a gap in being able to easily obtain metric information which is crucial for decision making- this project is stuck with Integrated Digital Services, which is difficult. (City Development)

Regarding this comment, Integrated Digital Services Digital Change will contact City Development to review the projects underway to understand which project is referred to as stuck.

Principle 6: Developing Capacity.

b. Integrated Digital Services and HR processes seem to be different depending on who you are liaising with. Support is good when it's available but inconsistent. HR/Management involves too much resilience on managers where specialist support would be more efficient; Integrated Digital Services seem under-resourced. (Strategy and Resources).

The comment regarding Integrated Digital Services being under-resourced is being addressed through a new IDS Resource Augmentation Framework which the Director of Strategy and Resources approved the award of contract to the following suppliers.

Lot 1: Digital Engineering and Integration - Fujitsu - AireLogic
Lot 2: Digital Solutions and Automation - Fujitsu
Lot 3: Digital Transformation Consultancy - Fujitsu - AireLogic
Lot 4: Digital Experience and Design - Fujitsu - TPX Impact
Lot 5: IT Operations & Support Services - No awards being made.

The multi-year framework contract for resource augmentation within the Integrated Digital Service will run to the end of November 2026 with the option for a further 12-month extension.

The link to the framework decision can be found on this link Council and democracy (leeds.gov.uk). Reference D56934

c. Arrangements for governance of Integrated Digital Services - there has been little strategic oversight of our Integrated Digital Services plans for the last 3 years or so and so the service has limited understanding or influence over Integrated Digital Services developments specific to the service, meaning that we are not as competitive, efficient, or effective as we should be. Business Partner arrangements have been ineffective for the last 2-3 years. Our arrangements for staff induction could be stronger. Review underway. (Communities, Housing and Environment)

Integrated Digital Services have moved to a Product Management approach, which has replaced the previous Business Partnering arrangements. Business Partnering is a component part of Product Management, as is Service Management. It is clear from this comment that the CHE directorate feel there is currently a gap around strategic oversight of the directorates plans. Integrated Digital Services Senior Leadership Team will review partnering arrangements with CHE to put in place support arrangements to address this.

Learning from the survey

49. It was commented that there is an overreliance on Integrated Digital Services for Business Continuity without services understanding how they would operate without a Digital service for a period. This will need picking up with the Corporate Risk team to ensure that BC plans are fully developed in services which cover off on Digital.

50. There were further comments about how a communication plan would work if the majority of staff were working from home, this will need developing with the Corporate Risk team as part of Business Continuity planning for Integrated Digital Services.

51. It was perceived that risks were not properly being identified with Integrated Digital Services and communicated. As explained elsewhere in this report risks are reported quarterly on two specific risks. However more granular risk reporting may be appropriate.

52. Comments were made that the way information on new services and technologies being deployed was drip fed and that Insite toolkits were out of date, this will need picking up with Digital Change to ensure deployments of products and new technologies is improved to ensure the business are aware of new developments and have the knowledge and training to use them effectively.

53. It was identified that the relationship between the Business and Integrated Digital Services is too distant and needs improving to make the interface better. Work is underway on the new Integrated Digital Services structure which includes the Digital Change team which will work closely with the business to ensure they have the right support to achieve their digital ambitions.

54. It was also mentioned that Integrated Digital Services struggles with capacity and therefore is unable to achieve the outcomes required by business areas. This is recognised and is being addresses through augmenting Integrated Digital Services teams with technology partners in specific areas (PowerApps, Robotic Process Automation) and though offshoring to bring in technical staff to support teams.

Statement of Assurance

55. Having undertaken the review of the system of internal control for Integrated Digital Services outlined in this statement the Director of Resources is satisfied that the arrangements are up to date and fit for purpose, that they are communicated and embedded and that they are routinely complied with.

56. However, given the feedback from the Internal Control survey, organisation design changes, and the move to a more integrated approach to support services, it is likely that the next year will see some changes and further improvements.

57. The Director of Strategy & Resources & Chief Digital & Information Officer have identified the following opportunities for enhancement of the system of internal control for decision making and will implement these over the course of the 2024/25 municipal year.

Opportunities for improvement

Define and Document	Complete work on documentation of key Integrated Digital Services Strategies.
Clearly Communicate	Complete the work on the Digital Communication Plan.
Effectively Embed	Complete work on the development of Digital Roadmaps.
Meaningfully Monitor	Review existing KPI's to ensure fit for purpose and add new ones if required. Review Quality Assurance arrangements for the service.
Review and Refine	Review how risks are identified and reported. Complete the recommendations identified in the Cyber Security Risk Management audit. Internal Audit review of the governance on the Essential Services Programme. Internal Audit Privilege User access control review.

Report author: Aaron Linden and Shona McFarlane

Annual Information Governance Report, including the Annual Report of the Caldicott Guardian

Date: 12th February 2024

Report of: Director of Strategy and Resources and the Director of Adults and Health

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

Brief summary

This annual report presents assurances to the Corporate Governance & Audit Committee on the effectiveness of the council's information management and governance arrangements through a statement of internal control.

In addition, the report this year presents the Information Commissioner's Office (ICO) Audit Report of Leeds City Council's compliance with the UK General Data Protection Regulation (GDPR), for which Members are to be assured that an action plan is in place to address the recommendations.

The Caldicott Guardian gives assurance to Members of the arrangements in place with regards to the confidentiality of patient and service-user data.

Recommendations

Members are asked to:

a) Consider the contents of this report and the assurances provided within the Council's Corporate Information Management and Governance Statement of Internal Control.

b) Note the outcome of the ICO Data Protection Audit, acknowledging the areas for improvement, and agree to receive mid-year and end of year action plan progress update reports.

What is this report about?

1 This annual report presents assurances to the Corporate Governance & Audit Committee on the effectiveness of the council's information management and governance arrangements: that they are up to date; fit for purpose; effectively communicated and routinely complied with, as well as arrangements that are in review or development to keep pace with developing risks or changes to legislation and guidance. See Appendix 1.

2 In addition, the report this year presents the Information Commissioner's Office (ICO) Audit Report of Leeds City Council compliance with the UK General Data Protection Regulation (UK GDPR). See Appendix 2.

3 The ICO Audit looked at 3 key areas and the assurance ratings received by the Council are as per the table below. The available assurance ratings were; Very limited assurance, limited assurance, reasonable assurance, and high assurance. We welcome the views of the ICO and appreciate the support they have given us. Whilst accepting that there are areas for improvement, we are encouraged that many were known to us and were already included in the Information Management and Governance Work Programme.

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Personal Data Breach Management and Reporting	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

4 The ICO will be undertaking a follow up audit during December 2024.

5 Members are to be assured that an action plan is in place to address the recommendations and Officers wish to keep Members up to date with progress.

6 A number of existing controls detailed in Appendix 1 will be further improved as part of the ICO Audit Action Plan to provide the Council with greater controls and great assurance mechanisms.

7 The Caldicott Guardian gives assurance to Committee of the arrangements in place with regards to the confidentiality of patient and service-user data.

What impact will this proposal have?

8 The council processes a considerable amount of citizen data and has a duty to process this data in accordance with legislation, government standards and good practice. Effective corporate information management and governance arrangements should help prevent risks arising or mitigate their impact on citizens should they occur.

9 As well as continuing with ‘Business-as-usual' activities and pre-identified areas for continuous improvement, of which many have been acknowledged within the ICO Audit Report, meeting the terms of the recommendations will increase the Council’s information management and governance maturity.

How does this proposal impact the three pillars of the Best City Ambition?

☒ Health and Wellbeing ☒ Inclusive Growth ☒ Zero Carbon

10 Appropriate collection, storage, use, security and sharing of information supports each of the council’s three Key Pillars. Each pillar requires information and therefore poor information management and governance practices could impact on their achievement. The information management and governance arrangements aim to ensure that all council information is managed appropriate, lawfully, and safely.

What consultation and engagement has taken place?

Wards affected: N/A

Have ward members been consulted? ☐ Yes ☒ No

11 Consultation on the development of strategies, policies, procedures and standards are undertaken across a broad range of stakeholders including information management professionals, representatives from all Directorates via the Information Management Sterring Group, People and Culture Board and elected members.

12 The Information Management and Governance (IM&G) management team continue to meet with the ICO Group Manager for Freedom of Information (FOI) casework on a bi-annual basis, who the Council is actively engaging with.

What are the resource implications?

13 The systems and processes in place and described within this assurance report have been established to manage the allocation of resources and to manage resource conflicts.

14 The efforts required to meet the requirements of the ICO Audit Recommendations will be substantial whilst maintaining the existing service provision and progressing existing projects. However, with appropriate links into the People and Culture Board (see Appendix 1, Section 2.2 and Section 12), any unmanageable pressures will be reported and managed.

What are the key risks and how are they being managed?

15 Failure to embed an effective Information Management and Governance Framework with appropriate policies, procedures, risk management, reporting, auditing and associated continuous improvement work programme could result in non-compliance with the UK GDPR, the Data Protection Act 2018 (DPA18) and the Freedom of Information Act (FOIA) as well as associated Codes of Practice and guidance. This could lead to data breaches which could cause harm to individuals that in turn could lead to complaints, compensation claims and a loss of confidence in the Council by citizens, partners, contractors and other third parties. In addition, this could lead to regulatory action from the ICO including fines and reprimands.

16 There is a corporate risk associated with Information Governance; LCC 26 - Information Management and Governance.

17 Several associated Directorate level IM&G risks are also managed. All risks are articulated in full in section 9 of Appendix 1.

18 There is also a statutory performance related risk on the council's failure to meet legal time limits for responding to information right requests. With improved performance over the last 7 months and the development of a new Power App to improve our process further, our aim remains to remove/reduce this risk during 2023/24.

19 There is a related risk of non-compliance with Public Services Network (PSN) standards which could leave the Council vulnerable to a number of impacts. This is however covered in the wider Update Report on IDS Governance.

20 Non-compliance with the Caldicott function could leave the Council vulnerable to the following risks:

a) compromises to the security of confidential person/ patient identifiable data.
b) damage to the Council's reputation and the trust which individuals place in the Council to safeguard their data.
c) infringements of data protection legislation / law on confidentiality and subsequent complaints / claims from individuals affected.
d) non-compliance with the Data Security and Protection toolkit which would restrict the sharing of patient data with the NHS.
e) enforcement action from the Information Commissioner's Office.

21 All risks are managed through the Council's Information Governance and Risk Framework which consists of appropriate policies, procedures, risk management, reporting, auditing and associated continuous improvement work programme, which will be further improved through implementation of the ICO Audit Recommendations.

What are the legal implications?

22 It is a legal requirement to comply with the UK GDPR, the DPA18 and the FOIA, as well as associated Codes of Practice and guidance.

Options, timescales and measuring success

What other options were considered?

23 N/A

How will success be measured?

24 Success will be measured through the Council's corporate KPI and future benchmarking with neighbouring and/ or Core City local authorities. Success will also be measured with an appropriate Information Assurance Framework, following the implementation of the ICO Audit Recommendations

What is the timetable and who will be responsible for implementation?

25 General information management and governance arrangements are ongoing. However, the deadline for the ICO Audit Recommendations to be completed is by December 2024.

26 The Head of Information Management and Governance is responsible for ensuring the ongoing appropriateness of information management and governance arrangements and for meeting the deadline for the ICO Audit recommendations to be completed.

Appendices

- Appendix 1 - Corporate Information Management and Governance Statement of Internal Control
- Appendix 2: Leeds City Council – ICO Data Protection Audit Report

Background papers

- N/A

This page is intentionally left blank

APPENDIX 1 – Corporate Information Management and Governance Statement of Internal Control

Define and Document

1. Information Management and Governance Policies and Procedures

Policy	Protocol	Procedures
Information Compliance Policy • Data Protection Policy Statement • Freedom of Information and Environmental Information Regulations Policy	• Filming and Photography Protocol	• General Data Protection Regulation (GDPR) Toolkit • Toolkit for managers of leavers and movers • International Transfers – Practitioners Guide • Looking after information Toolkit • Information Requests Toolkit
Data Quality Policy	N/A	N/A
Information Assurance Policy • Remote Working Policy • ICT Equipment Disposal Policy	• Acceptable Use Protocol • Password Protocol • Information Security Incident Protocol	• Encrypted memory sticks Toolkit • ICT Equipment Disposal Procedure • Procedure for the Secure Storage of Filing Cabinet Keys (Children's and Adult Social Care only) • Procedure for Taking Personal Data and Special Category Data Off LCC Premises (Children's and Adult Social Care only) • IMG Training Strategy • Information Incident toolkit
Information Sharing Policy	International Transfers protocol	• Sharing information Toolkit • High Security File Transfer Procedure • Sharing Information for research Projects Procedure • Peer Checking for Post Procedure
Records Management Policy • ICT Back-up Retention Policy	Office Move Protocol	• When and how to dispose of information Toolkit • Using the records management facility Toolkit • Track and Trace Procedure for Hard Copy Files • Creation, storage, and disposal of information Toolkit

2. Roles and Responsibilities

2.1. Decision making

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Director of Strategy and Resources			
HMG Security Policy Framework Version 1.1 – May 2018	Undertake role of Senior Information Risk Owner (SIRO)	Chief Digital and Information Officer	Where the SIRO is not available: have ultimate responsibility for the acceptance, or otherwise, of information risks for the council; responsible for approving, and ensuring implementation of, all policies and procedures relating to the Information Governance Framework
HMG Security Policy Framework Version 1.1 – May 2018	To approve Information Governance (IG) policy exemptions	Chief Digital and Information Officer	Level 3 exemptions where it is anticipated there will be a high business impact. In consultation with Information Management Steering Group and People and Culture Board. Level 1 and 2 exemptions where it is anticipated there will be a low or medium business impact. In consultation with key stakeholders
HMG Security Policy Framework Version 1.1 – May 2018	To investigate information security breaches	Chief Digital and Information Officer	In liaison with HR and other key stakeholders
HMG Security Policy Framework Version 1.1 – May 2018	Approve Information Sharing Agreements, Data Processing Agreements, Non-disclosure agreements when sharing information with third parties	Information Asset Owners	For the information assets for which they have been identified as the responsible officer
		Information Governance Officers in relation to matters within their remit	Where the relevant IAO is not available
Director of Adults and Health			
Local Authority Circular (2002) 2	To act as Caldicott Guardian for Adult Social Care	Deputy Director Social Work and Social Care Services	For matters relating to Adult Social Services

Place from where function derived	Function Delegated	Officer to whom delegated	Terms and Conditions
Implementing the Caldicott Standard into Social Care	To act as Caldicott Guardian for Public Health	Director of Public Health	For matters relating to Public Health and to sub-delegate as necessary
	To act as Caldicott Guardian for Children's Services	Director of Children's Services	For matters relating to Children's Services and to sub-delegate as necessary
Data Protection Officer			
DPA (Data Protection Act) 2018 and UK GDPR (UK General Data Protection Regulation)	N/A	N/A	The Head of Information Management and Governance is the Council's Data Protection Officer (DPO). The DPA 2018 and UK GDPR requires the council, as a public authority, to designate a Data Protection Officer. The main tasks of the DPO are: to inform and advise the council of its obligations under UK GDPR when processing personal data; to monitor compliance with the UK GDPR; to provide advice where requested, particularly, with regards to data protection impact assessments and other high risk processing activities; and to act as the contact point with the supervisory authority (the Information Commissioners Office (ICO)).

2.2. Leadership and Oversight

Democratic Oversight	
Executive Member for Strategy and Resources	Oversight of executive decision making with regards to IM&G
Corporate Governance and Audit Committee	Annual Information Governance Reporting, including the Annual Report of the Caldicott Guardian Ad hoc reporting on request of the Committee, for example: • PSN Compliance • International Transfers and Data Adequacy • Access Project

Strategy and Resources Scrutiny	Ad hoc reporting on request of the Committee, for example: • Performance with regards to Freedom of Information Requests
Management Oversight	
People and Culture Board	Providing leadership, oversight and an approval mechanism for Information Governance Policy.
Information Management Steering Group	Chaired by the Head of Information Management and Governance (DPO)The purpose of this Steering Group is: • Support and put into operation, the Information Management Strategy by delivering on associated projects and work items, and to assess compliance with the Council's assurance standards on behalf of the Data Protection Officer. • Ensuring that an appropriate comprehensive Information Governance and Cyber framework and systems are in place throughout the Council. • Monitoring a cycle of information and data management improvements in a way that is compliant with the law and in line with national standards. • Providing assurance to the Council's Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO) in relation to the Council's arrangements for creating, collecting, storing, safeguarding, disseminating, sharing, using and disposing of information in accordance with its: o stated objectives / purposes. o legislative responsibilities o risk appetite • Providing strategic leadership and direction on Information Governance, Information Risk and Cyber work prioritisation and provide assurances to key stakeholders. With a Strategic and Corporate reporting line into People and Culture, the Information Management Steering Group has replaced the operational aspects of Information Assurance Board and has consumed the previous Records Management and Policy Review Sub-Groups. The Data Practitioners Group continues and will report into the Steering Group to ensure appropriate awareness of the need to respond to changes in legislation and regulation. A sub-network of Information Asset Owners has also been established as part of the Steering Group to enable the operational aims and tasks of the Steering Group to be implemented and to allow for two-way feedback.
Data Practitioners Group	Chaired by Legal Services. The purpose of this Group is: • looking at and responding to consultations; • reviewing new ICO guidance / codes of practice; • reviewing recent case law • reviewing ICO decisions

3. Communication

Format	Outline
Leadership	The SIRO is corporately responsible for Information Risk. The SIRO communicates to all employees on high-risk matters and on compliance matters such as training. The DPO is corporately responsible for informing and advising the Council of its obligations under UK Data Protection legislation when processing personal data; to monitor compliance with the GDPR; to provide advice where required, particularly, with regards to data protection impact assessments and other high risk processing activities; and to act as the contact point with the supervisory authority (the Information Commissioners Office (ICO)). The DPO meets with the SIRO monthly. The DPO communicates to all staff via the Managing Information Toolkit on InSIte. At a more local level in Information Management and Governance, communication takes place in weekly Management Team Meetings and the DPO Forum, and information is cascaded to all members of staff, as appropriate in a weekly messages meeting.
Training	There is an Information Governance Training Strategy. The was last reviewed and approved by Information Management Board in February 2020, with a light touch review undertaken in April 2022. As part of the ICO audit review the IMG training strategy will be reviewed and updated to reflect the recommendations made by the ICO. Currently, the strategy documents the training requirements of all those who work for or on behalf of LCC including those on temporary contracts, secondments, volunteers, elected members, students and any staff working on an individual contractor basis and/or who are employees for an organisation contracted to provide services to LCC. The strategy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions. There are four levels of training which are described below: **Level 1.** All LCC staff are mandated to undertake this basic training in Information Governance. Training is available through two channels; • an e-learning package for PC users, • a brochure or leaflet for other staff. The Level 1 training is generic and covers IG related legislation, local policies and information security. **Level 2.** This is targeted at staff who have access to special category information as part of their everyday duties. It consists of several packages each tailored to the issues specific to a policy/service area. These packages; • build on the Level 1 training, • are classroom based, ‘face to face’ and interactive (these have been conducted remotely during the pandemic).

Format	Outline
	They provide staff with a high level of understanding about appropriate data handling and their own responsibilities when handling council information. **Level 3.** Bespoke training packages are developed and delivered to implement specific information governance programmes of work such as; • the responsibilities of Information Asset Owners • Cyber – Exercise in a Box & Hacking and Cracking training • Records Management • Data Protection Such packages may be supplemented by briefings, discussion groups and newsletters. Subject Matter Experts may be bought in, or staff may attend external training courses or events. **Level 4.** The following positions within the Council have the 'expert' level training necessary to provide the roles. This training is commissioned for the individuals as and when required and is usually provided by an external training provider: • SIRO - To assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties. • Caldicott Guardian - To fully understand the role and function of the Caldicott Guardian. • Data Protection Officer - In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security. • IDS Security lead - In depth understanding of the General Data Protection Regulation and Data Protection Act (and associated legislation) and information security. n depth understanding of all technical information security and assurance. All staff will have on-going refresher training, the level and frequency of which will be decided on an individual/service area/need basis. Level 1 refresher training is mandatory and will be undertaken at least every two years.
Guidance	The Managing Information Toolkit on InSite provides access to guidance, procedures and instruction for all employees covering the following areas: • Creation, storage and disposal of information • GDPR • Information about managing staff records • Information security incidents • Looking after information • What to do if you receive a request for information • Sharing information

Format	Outline
	• Using the Records Management Facility • When and how to dispose of information • Information management and governance policies

4. Statutory and non-statutory information requests

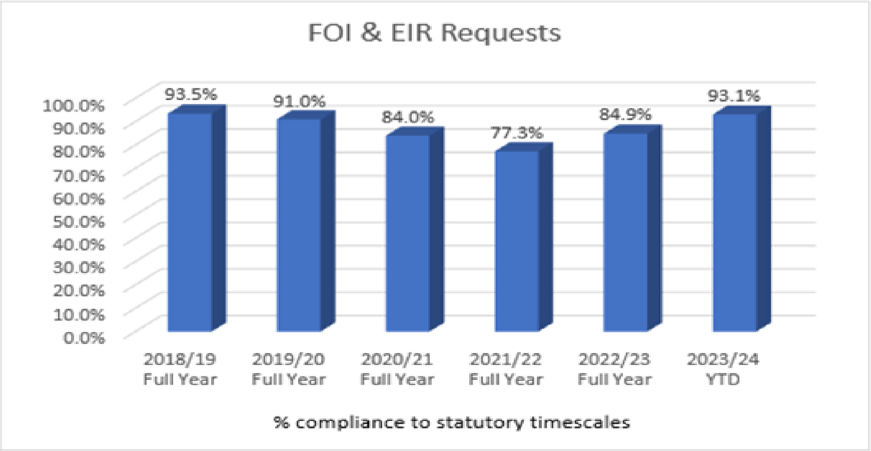
4.1. Data protection law gives individuals greater control over their personal data through several rights. Individuals are informed of their rights through the Leeds City Council Privacy notice available on our website. All staff are made aware of these rights through the information governance e-learning level 1 and information governance policies and procedures.

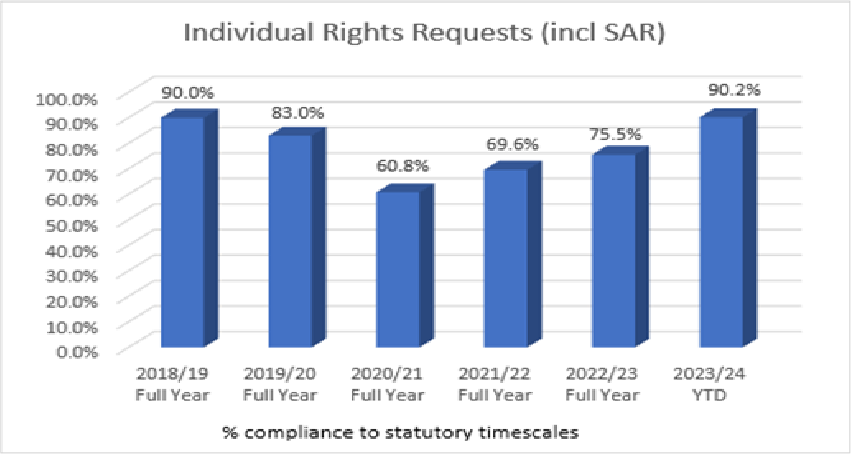
4.2. The IM&G service is responsible for processing and responding to all information requests to the council. This includes those made under the Freedom of Information Act 2000 (FOIAs) and the Environmental Information Regulations 2004 (EIRs), the UK General Data Protection Regulation (GDPR) (Individual Rights Requests – IRRs including subject access requests) and the UK Data Protection Act 2018 (including requests from the police, the courts, partner agencies and other government bodies and regulators).

4.3. The UK GDPR stipulates that Subject Access Requests (SARs) must be responded to within one calendar month from receipt of the request (or two additional months if the request is complex or voluminous). The Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR) set the statutory timeframe for responding to requests at 20 working days from receipt of the request.

4.4. The KPI for FOI/EIR requests is currently to respond to 90% of requests within the statutory time limits. The KPI for IRRs is presently set at 88% of requests responded to within statutory timeframes. As the IM&G requests team deals with all statutory requests to the council, performance for these two indicators is closely linked.

4.5. The charts below set out the number of statutory requests received and handled by the council within the statutory timeframes from 2018/19 to 2023/24, with figures provided for 2023/2024 being year to date up until 29th December 2023. As per the detail provided at table 3.9, performance is on course to not only be improved, but to exceed our currently set KPIs.





s

Number of requests	2018/19 Full Year	2019/20 Full Year	2020/21 Full Year	2021/22 Full Year	2022/23 Full Year	2023/24 YTD*
FOI & EIR Requests	2455	2535	2158	2024	2039	1594
Individual Rights Requests (Incl SARs)	855	949	717	751	929	767

*Year to date

4.6. Performance in both areas is strong and improved from last year and previous years, even though there has been an increase in FOI/EIR/IRR requests when compared to the same period last year (see 3.9 for more details). Moreover, all request streams are now above the council's KPIs due to a change in operational ways of working within the Information Management and Governance Team, but also due to a revised way of working together with services over the last 18 months. Whilst the council is exceeding targets and performance has improved, the FOI/EIR KPI is currently below the ICO's expected level of 95% and the IM&G service are on a journey to reach that for financial year 24/25.

4.7. Development work also is progressing with colleagues in IDS to create the council's new information request Power App. The Power App will bring automation and efficiencies to the administration of requests within the IM&G service and the wider council. It is anticipated that the new Power App will be launched with the business during Q1 24/25.

4.8. In addition to the new Power App, the IM&G service are looking to procure redaction software to replace Adobe Pro that is currently used by several services across the council. The current tools and processing around redaction are dated and have not kept pace with other technology tools and processes on the market, which offer far more efficiencies and safeguards. It is manual, time-consuming, and prone to user error. There is an increasing need for innovative technologies (alongside improved guidance and support for staff) to improve consistency and streamline the redaction process and the new redaction software will need to work alongside the new requests Power App. Market research and soft marketing testing has commenced, with the aim of procuring the software before the end of the current financial year.

4.9. Summary of Requests Received

Individual Rights Requests	As at 29th December 2023, the council has received 767 Individual Rights Requests (IRRs) in the first 3 quarters of the financial year 2023/24 and the majority of these are subject access requests (SARs). The council has seen a 15% increase in the number of IRRs received in the 2023/24 financial year to date compared to the same period last year. 29% of IRRs for this year to date are for access to children's social care records by individuals who were in care, or from the parents whose family have social care involvement. Due to the sensitive nature of these records the requests are highly complex and frequently run into thousands of pages. Currently, every page must be read, and decisions then made in respect of applying any necessary redactions as provided for in the UK GDPR/DPA, with some extremely difficult information to be reviewed in respect of child protection matters. The procurement of a redaction software solution will enable staff to automate redactions across thousands of pages which will improve the quality of redactions and reduce the risk of manual errors (which can lead to data breaches).
Freedom of Information/ Environmental Information Regulations requests	The council has received 1594 Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests in the first 3 quarters of the 2023/24 financial year, which represents a 9% increase when compared to the same period last year. The IM&G service are responsible for logging and coordinating the identification and collection of information requested, preparing the final response, and identifying and applying any exemptions from the relevant legislation, as well as liaising with services and the corporate communications team regarding any high-profile requests before they are disclosed.
Police, Court & CCTV Requests	The IM&G service also processes and responds to on average 2000 requests per year from the police, other local authorities, HMRC, court orders and the Home Office for access to information, primarily to assist in the prevention, investigation, detection or prosecution of criminal offences. This includes Annex C requests where the Police undertake enquiries linked to historical or current alleged physical or sexual abuse of children. The number of requests received and responded to by the IM&G service has been consistent over the last 4 years with no indicators to show that the volume of these requests will reduce. These requests vary in their complexity from an address check, to arranging access to social care records, which involves access to

	paper and electronic files. The time taken to process police requests is significant and is supported from an administration perspective by the team at Westland Road.

ICO & Internal review cases

4.10. If a requester is unhappy with the initial response to, or handling of their request, they can ask for an internal review which is dealt with as a stage 2 complaint under the council's complaints policy. To date this financial year the council has received 88 internal review requests for IRRs/FOIs/EIRs. This is comparable with last year's figures for the same period.

4.11. Requesters are thereafter able to appeal to the Information Commissioner's Office (ICO) if they have concerns about the way the council has responded to their complaint. In this financial year to date, 13 requesters have submitted appeals against the council to the ICO.

4.12. Whilst the council has seen an overall 11% increase in the number of FOI/EIR/IRR requests received when compared to the first 3 quarters of last year, the number of ICO cases represents a 28% decrease in appeals to the ICO when compared with the same period last year. In addition, none of the ICO cases made against the council this year have been fully upheld (see 3.15 for more details).

4.13. As with internal reviews, a substantial amount of capacity is required to respond to ICO appeals as these tend, by their very nature, to be complex and often span a considerable time limit of involvement with the council.

4.14. Of the 13 cases submitted to the ICO this year to date, the council currently has no open ICO cases awaiting an ICO finding. The outcomes of the 13 cases received to date this year are summarised below. Where the ICO agrees with the council's handling of a request, this would be determined as not upheld. Where cases are either partially or fully upheld, IM&G have processes in place to ensure the council learn from these.

Not Upheld – no decision notice issued (IRRs only)	5
Not Upheld - decision notice issued (FOI/EIRs only)	4
Partially upheld (IRRs only)	4
Upheld	0
Waiting on ICO decision	0

4.15. Of the 4 cases partially upheld, the ICO determined that the council either did not provide a response to the request within the statutory timescales and/or determined that the council had further work to do in respect of these requests, e.g. review if all information was released.

5. Records of Processing Activities

5.1. It is a legal requirement that the processing activities of the Council are documented. The Council does this through its Information Asset Register and Record of Processing forms, which are used to inform the asset register.

5.2. Within the information asset register the following requirements are included:

- Information Asset Owner (directorate and service).
- Name and purpose of asset.
- Categories of personal data/special category data.
- Format it is in, where it is stored, access permissions and volume.
- Retention details.
- If it is shared, internationally transferred or hosted.
- How critical it is and its risk rating.

5.3. The Council has identified over 1,500 information assets council wide, and 30 Information Asset Owners (IAO) have received reports/presentations regarding the status of their assets. Further work has been done to confirm Information Asset Owners, following staff leaving and service names changes. Awareness sessions have taken place to inform the IAOs of their role and responsibilities and discuss further developments to the asset register. Work has also begun to classify data against the Local Government Classification Scheme. Following this phase of the Information Asset Register implementation, work will commence on updating the register following the move of data to cloud platforms, producing a dashboard for reporting to the SIRO and linking the assets with the ROPA forms, to provide a holistic picture of data assets and their associated processing activities.

5.4. It is envisaged the above tasks will be completed by the end of March 2024. A review of the Information Asset Register will be completed as part of an overall information management programme, engaging with each service area individually. The annual review of the Information Asset Register by Information Asset Owners will then commence in 2025/26.

6. Data Protection by Design and Default

6.1. Leeds City Council requires that Data Protection Impact Assessments (DPIAs) be undertaken whenever there is processing of personal information, regardless of the level of risk presented. This is a higher threshold than is required under UK legislation (UK GDPR Article 35(1) states that that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals).

6.2. IM&G is completing a project to review and update the current corporate DPIA form, procedure and case management system in line with Internal Audit’s recommendations. The overall objective of the review is to provide assurance that there are appropriate controls in place to ensure that DPIAs are completed where required.

6.3. The review has incorporated the development of a new system, utilising the Power Apps platform, that will enable the monitoring of DPIAs by IM&G throughout the entire lifecycle of a project from project creation to closure. It will also enable information governance risks to be identified, monitored, and signed off by the relevant information asset owner. The system will enable DPIAs to be linked with the information asset register in the future (subject to further development taking place).

6.4. It is intended that the new DPIA form and system will be launched in Q4 2023/24 and will be supported by bi-annual comms to all council staff, reminding them of the need to complete DPIAs and to highlight the published forms/procedures/guidance available.

7. Records Management

Paper Rationalisation Programme/Office Asset Rationalisation

7.1. IM&G have, this year, assisted Asset Management with the following office closures, Adams Court, Farnley Hall, Lavendar Walk and Broomhill Family Centre, ensuring rationalisation of their paper records, including destruction and archiving and ensuring paper records are removed from the buildings to avoid a security incident once the buildings are sold.

7.2. IM&G will undertake an audit as part of the information management programme to ensure all paper records across the organisation, have been accounted, recorded and are being managed appropriately, particularly considering the move to home working.

7.3. IM&G work in partnership with the Corporate Records Management Facility (CRMF) to ensure the secure and appropriate management of our archived records. This has included the implementation of a new SharePoint system to support the management of the records, for both archive inputting and searching and requesting records. Work continues to move the CRMF SharePoint site to the cloud. This is required for two reasons, firstly as the current site is not performing at its optimum, reporting is not adequate, and performance is slow. Secondly SharePoint 2013 will be out of support during 2023, therefore, the site needs to be moved elsewhere. We continue to work the facility to ensure destructions of paper records beyond their retention are carried out to meet our statutory obligations of not holding data for longer than is necessary and to free space up at the facility. We are still supporting the facility in coming out of a third-party record storage provider and moving the data to a new provider.

7.4. The council have a scanning framework with Restore Digital to provide scanning contracts where needed across the organisation. Any paper rationalisation work will also look to see where there are digitisation opportunities which may require scanning of records.

Microsoft 365 and Retention

7.5. IM&G and wider IDS colleagues have undertaken discovery work to understand the information management capabilities within M365. There have been successful feasibility tests in relation to how, for example, Syntex (a capability within M365) can label data. Over the coming year the Information Asset Register will be mapped against the corporate retention schedule and information assets will be classified in line with the Local Government Classification Scheme. IM&G staff and wider IDS staff have been looking at using classifiers to label data using M365 Syntex tool. Once data is labelled, M365 Purview will be used to apply retention policies to the labels, ensuring data is being managed in accordance with GDPR principle of data minimisation and storage limitation.

7.6. Data remaining in NetApp file stores will be analysed to determine data which requires archiving, and which can be destroyed. A cloud-based archive solution will be implemented with information management capabilities as an essential requirement. Any data required for permanent preservation will be offered to West Yorkshire Archive Service. An archive solution will also be considered for data from decommissioned systems which needs to be kept for retention purposes beyond the life of the application.

8. Caldicott Guardian

8.1. In August 2021, the National Data Guardian issued guidance on the appointment of Caldicott Guardians, their role and responsibilities in respect of data processing activities undertaken within their organisations. As it is published, under the National Data Guardian's power to issue guidance described within the Health and Social Care (National Data Guardian) Act 2018, those organisations that it applies to need to give it due regard. The guidance underlines that the relationship between with the Caldicott Guardians and other information governance professionals within an organisation and with decision makers is very important.

8.2. The council's Caldicott Guardian and delegates receive a quarterly performance report from the IM&G service, covering all aspects of information governance, including directorate projects, information security incidents and information rights requests.

9. Corporate and Directorate Level Risks

Probability	Impact	Risk Score	Controls
LCC 26 - Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and the council because of non-compliance with Information Governance legislation and industry standards.			
3 - Possible	3 - Moderate	High	The City Council's controls aimed at mitigating the Information Management Risk are evidenced in: (a) the Information Governance Framework; (b) the policies made under it (for example, the Information Security Policy); (c) other rules and Codes of Conduct; (d) Information Technology systems which contain or provide access to Council information; (e) physical asset protection measures; (f) other, system or risk specific, controls. (g) staff training on induction and every 2 years.
AH 12 - Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and the council because of non-compliance with IG legislation and industry standards.			
3 - Possible	3 - Moderate	High	- Mandatory IG training for all LCC staff - Data security and protection toolkit - IM&G Service - appropriately trained and skilled - IG Policies and procedures- rolled out, embedded and easily accessed within the directorate - Peer checking - Compliance with the Legal framework - Steering Group - Caldicott guardian - Audit reviews (Internal and External e.g., CQC file review) - Information Asset Owners and Information Asset register - Inbuilt system controls e.g., access and security - Contractual obligations, terms and conditions around IG with 3rd parties - Physical security controls in place to prevent unauthorised access to information and to help ensure its securely held e.g., staff ID badge challenge, locked doors, swipe card access, records locked away securely etc - CIS Shielding policy - HR checks and procedures

Probability	Impact	Risk Score	Controls
			- Employee obligations e.g., contractual, Code of Conduct
CF 11 – Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and to the council because of non-compliance with IG legislation and industry standards.			
3 – Possible	3 – Moderate	High	- Mandatory IG training for all staff - Data security and protection toolkit - IM&G Service - appropriately trained and skilled - IG policies and procedures - rolled out, embedded and easily accessed within the directorate - Peer checking - Compliance with Legal framework - Steering group - Caldicott guardian - Audit reviews (internal and external) - Information asset owners - Information asset register - Inbuilt system controls e.g., access and security - Contractual obligations, terms and conditions around IG with 3rd parties - Physical security controls in place to prevent unauthorised access to information and to help ensure its securely held e.g., staff ID badge challenge, locked doors, swipe card access, records locked away securely etc - Mosaic Shielding policy (currently under review) Level 2 IG training for Children’s staff – this is mandatory for access to the Leeds Care Record - CareCert
RES 33 – Statutory Information Requests: Failure to meet the legal statutory time limits for responding to information rights requests (FOI/EIR/IRR requests)			
3 – Possible	3 - Moderate	High	– SharePoint dashboards created for all directorates to support services with the monitoring of all current and late requests – Weekly/monthly monitoring of performance within IM&G requests team – Creation/implementation of an IM&G SharePoint site to enable the IM&G requests team to manage and monitor day to day processing of information rights requests – Daily route of internal escalation established within IM&G to reduce late requests – IM&G management tier to prioritise and manage workloads and ensure appropriate resources in place to manage statutory information rights requests

Probability	**Impact**	**Risk Score**	**Controls**
			– Rolling program of change to review all operational processes relating to this area of work and to create standard operating procedures which will drive efficiencies in terms of the time taken to deal with information rights requests – The development of a multi-disciplinary workforce, intended to increase capacity to deal with information rights requests in a more efficient manner – IM&G staff have undertaken externally provided practitioner certificate training on UK GDPR/FOI/EIR legislation – Continuous staff development is in place for IM&G staff through its internal workforce development program – Creation and development of case management system for handling statutory requests – Planned procurement of redaction software
CD 18 - Information Management and Governance: Risk of harm to individuals, partners, organisations, third parties and the council because of non-compliance with IG legislation and industry standards.			
2 - Unlikely	3 - Moderate	Medium	The City Council's controls aimed at mitigating the Information Management Risk are evidenced in: (a) the Information Governance Framework (b) the policies made under it (for example, the Information Security Policy) (c) other rules and Codes of Conduct (d) Information Technology systems which contain or provide access to Council information (e) physical asset protection measures

Review and Refine

10. New Ways of Working

In Quarter 1 of 2023/ 2024, the Information Management and Governance Team underwent a transition to a new way of working with 3 workstreams. One workstream is primarily externally/ customer facing, the second is internally demand led with cyclical risk and assurance work, whilst the third workstream is designed to focus its effort on large corporate and IMG initiatives. Work is grouped by the type of work demand and not by function. This has not only contributed to developing a multi-disciplinary team, but to improved performance. This new way of working is the foundation for the future to ensure we not only become as efficient as possible, but that we continue to keep up to date with developing risks, legislation and best practice.

11. Compliance and Assurance Framework

A function of the information management and governance remit that will be focussed on towards the tail end of 2024, following the completion of the ICO action plan, is an appropriate Information Management and Governance Assurance Framework. This will involve reviewing existing checks, inspections and auditing activities across the Council, to bring them under one framework, and to make any required improvements. This will then enable better assurance reporting to Chief Officers, People and Culture Board, CLT and Corporate Governance and Audit Committee.

11. Level 1 Information Governance Training

The mandatory Level 1 Information Governance e-learning is updated and launched every two years and a lessons learned report is produced at the end of every iteration. Version 5 of the eLearning product was launched in September 2022. The Council target for 100% completion across all digital users who have access to the LCC infrastructure (excluding members) was achieved.

The IMG service will be launching the updated version of the Level 1 Information Governance training in September 2024. The training will contain updated scenarios and reflect the recommendations of the ICO Audit.

12. People and Culture Board

From a previous Information Management Board in 2022 to the evolution of a more corporate and strategic Information Assurance Board in 2023, in the pursuit of efficiency and best use of resources, Information Management and Governance now reports into the People and Culture Board formally on a quarterly basis, with the Head of Information Management as a permanent member. This meets the purpose of the Information Assurance Board with the right audience, just without the additional administrative burden and additional officer time to attend a further meeting. With a route into CLT through the Board, this will contribute to the Council's position that Information Management and Governance is everyone's responsibility.

12. Information Risk Policy

Work has begun on developing an Information Risk Policy with the Council's Intelligence and Policy Manager. Whilst this will be embedded within the Council's wider Risk Management Framework, this Policy, as supported by the ICO audit, is designed to acknowledge the key differences of business and information risk management. This will result in a Policy as well as Directorate and Corporate Information Risks that are more tangible and manageable going forward. This risk assessment process will follow the Council's business risk management schedule and result in quarter risk reviews and reports to Directorate management teams as well as to People and Culture, CLT and the Corporate Governance and Audit Committee.

This page is intentionally left blank

Leeds City Council

Data protection audit report

December 2023

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Leeds City Council (LCC) agreed to a consensual audit of its data protection practices in June 2023. ICO audit team managers completed a scoping call with LCC to further discuss their current data protection compliance levels and the appropriate scope areas on which to focus the audit.

The purpose of the audit is to provide the Information Commissioner and LCC with an independent assurance of the extent to which LCC, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of LCC's processing of personal data. The scope may take into account any data protection issues or risks which are specific to LCC, identified from ICO intelligence or LCC's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of LCC, the nature and extent of LCC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to LCC.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Records Management	The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
Personal Data Breach Management and Reporting	The extent to which the organisation has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate.

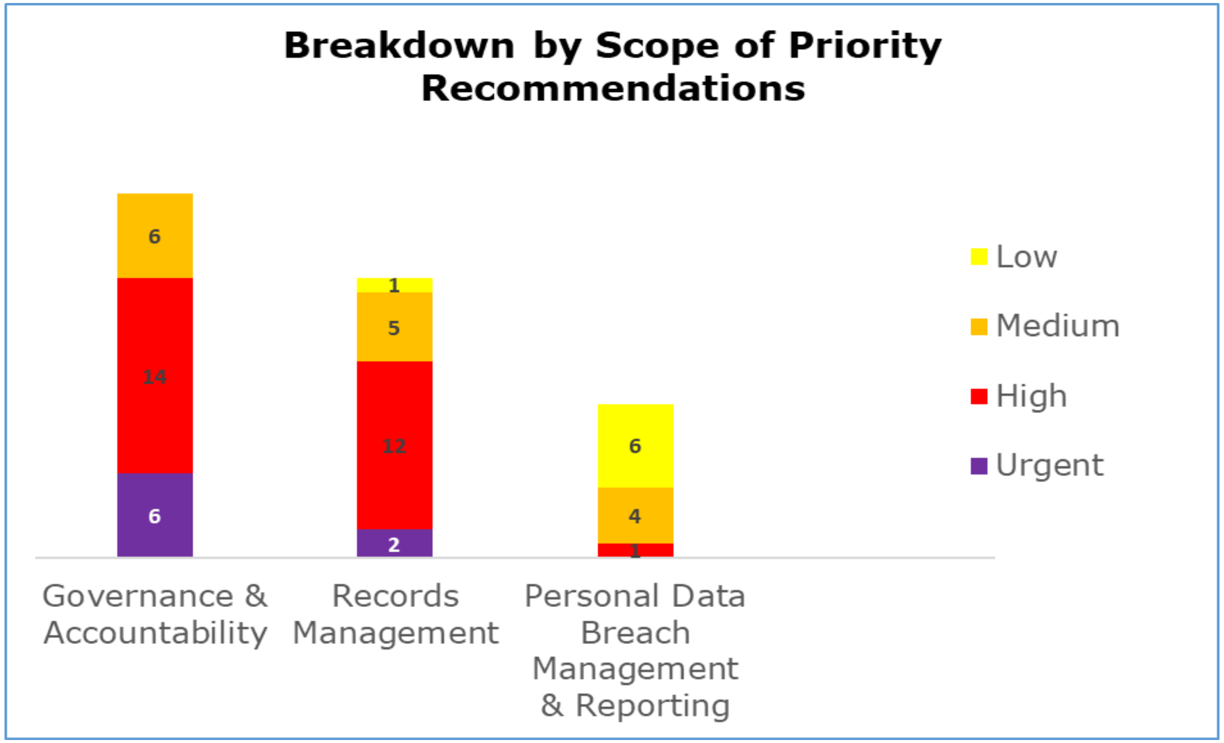
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential documentation.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. LCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Governance and Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Records Management	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Personal Data Breach Management and Reporting	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

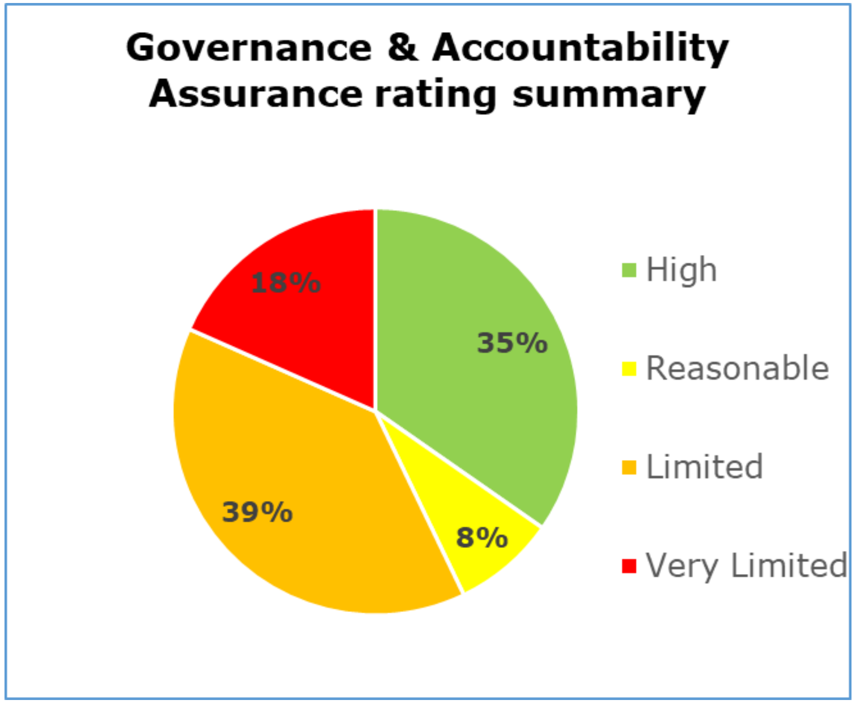
Priority Recommendations



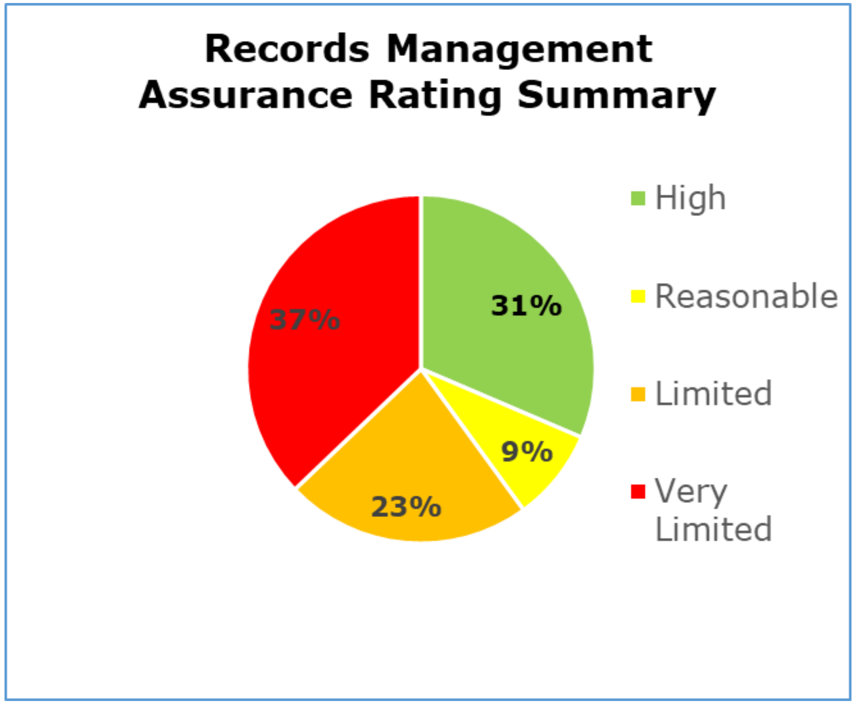
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has six urgent, 14 high, six medium and no low priority recommendations.
- Records Management has two urgent, 12 high, five medium and one low priority recommendation.
- Personal Data Breach Management and Reporting has no urgent, one high, four medium and six low priority recommendations.

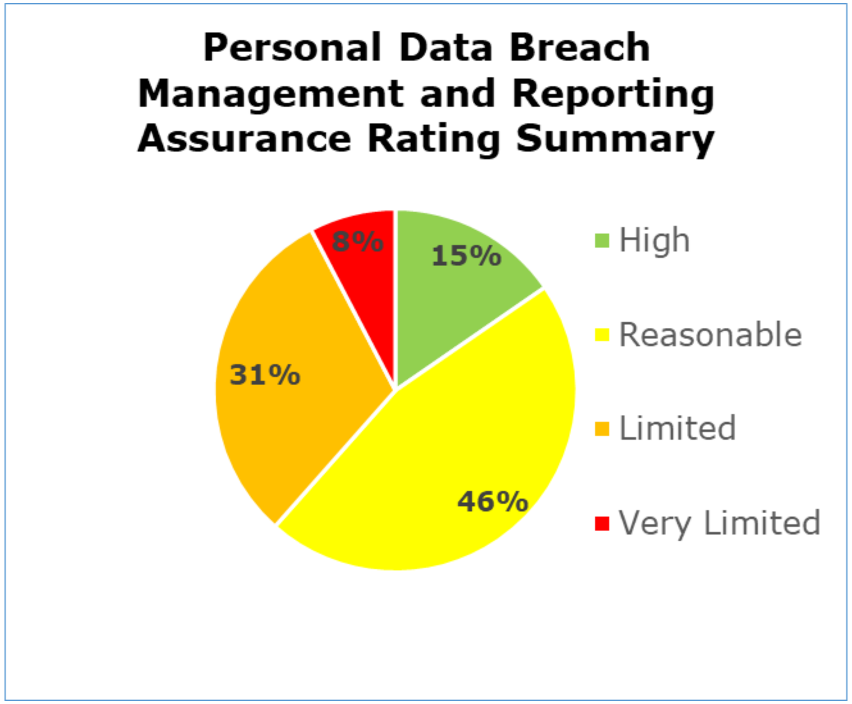
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 35% high assurance, 8% reasonable assurance, 39% limited assurance, 18% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 31% high assurance, 9% reasonable assurance, 23% limited assurance, 37% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Personal Data Breach Management and Reporting scope. 15% high assurance, 46% reasonable assurance, 31% limited assurance, 8% very limited assurance.

Areas for Improvement

Governance and Accountability:

- LCC must review, update, and create any missing Data Protection (DP) and Information Governance (IG) policies. These documents should be suitably extensive for the context of LCC and provide staff with sufficient direction that they are able to identify their roles and responsibilities.
- LCC should create an internal audit programme specific to DP with oversight and input from the Data Protection Officer (DPO). By implementing internal DP audits, LCC can gain assurance that their risk management is effective.
- LCC must create a centralised records of processing activities (RoPA) document. This will ensure LCC are in compliance with UK GDPR Article 30.
- LCC must conduct a review of their privacy notices to ensure that they include all the information required under Articles 13 & 14 of the UK GDPR. This will ensure that privacy information is sufficient to meet the legal requirements.

Records Management:

- LCC must complete an information audit and use it to inform their information asset register (IAR), RoPA and a weeding schedule and guidance. Without this, they cannot be assured they have full visibility of their information assets or the data quality of the assets.
- Disposal of excessive records is critical to UK GDPR compliance. LCC must create a full and relevant retention schedule and ensure there are sufficient processes in place to make sure this is enacted.

- LCC should ensure they have full and clear visibility of where data sharing has taken place and that appropriate contracts are in place. This will help processing of individual rights requests efficiently.
- There aren't consistent approaches to records management across the whole council which means that there's a risk of poor practice due to lack of clear guidance. Policies and guidance related to Records Management must be reviewed to ensure they are clear and cover everything required.

Personal Data Breach Management and Reporting:

- LCC should ensure that all decision makers within the IG team have received specialised training on Personal Data Breach Management and Reporting. This will ensure breaches are being accurately assessed and reported to the ICO where necessary.
- LCC should update the overarching retention documents to include retention periods, procedures and data minimisation techniques for the data breach logs. This will help LCC have an awareness of how often they should review breach logs and periodically reduce the personal information held within them.
- LCC should implement an alternate notification route in the case of a data breach that has been reported out of office hours. This will ensure that the council have appropriate procedures and guidance in place to maintain compliance.
- LCC should ensure all discussions held verbally or via email regarding reporting PDBs to the ICO are documented, e.g. decisions over not reporting a PDB to the ICO, the reason for any delays and any advice received from the supervisory authority.

Audit findings

The tables below identify areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a management framework, including a delegated process of accountability and responsibility from the Board down, to support the information governance management agendas.	A.01. Leeds City Council (LCC) have a documented information governance (IG) structure in place that outlines different IG roles such as the Head of information management and governance (IM&G), Records management lead, Resource and initiatives lead and IG officers. LCC have a senior information risk owner (SIRO) and deputy SIRO, however these roles aren't documented in the information governance structure provided. Furthermore, LCC do not have a management framework that documents information governance (IG) responsibility. The Head of IM&G is also the Data protection officer (DPO), however their job description (JD) does not include their DPO responsibilities. Furthermore, their JD states that it was last updated in March 2016. Without a clear management framework in	A.01. LCC must ensure that the reporting lines and flow of information between the Board and key individuals covering information governance management is documented. The overarching framework and strategy for information governance should be clearly outlined in policy documentation. LCC must also ensure that all senior management job descriptions and Board/ Committee terms of reference (ToR) outline IG responsibilities and designated accountabilities. They must be reviewed periodically to ensure they do not contain out of date information. This will provide LCC with assurance that there is effective and clearly defined oversight and management of information.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	place, there may be a lack of management focus on IG and data protection (DP). This can lead to senior management being unable to respond to breaches, and not being accountable for DP. This may result in non-compliance with UK GDPR Article 5(2).		
Operational roles and responsibilities have been assigned to support the day to day management of all aspects of information governance	A.02. LCC have an IG team who have the responsibility for the day to day management of DP compliance. The IG team are able to demonstrate their awareness and understanding of their role and responsibilities. LCC provided ICO auditors with copies of job descriptions for some of the IG team, including the Principal Information Governance Officer and Senior Information Governance Officer, which include their DP responsibilities. However, ICO auditors did not gain assurance that all DP responsibilities are included, for instance their Personal Data Breach (PDB) responsibilities, as they do not appear to have been reviewed or updated since April 2018. If LCC does not periodically review and update job descriptions, breaches may be caused by staff being unaware of all of their responsibilities. It can also lead to staff failing to carry out day to day, operational level DP practices.	A.02. LCC must review job descriptions for IG staff and update them where necessary, to ensure they clearly outline all their DP responsibilities. After the job descriptions are reviewed, they must be shared with the relevant individuals. This will help LCC gain assurance that staff in IG roles are able to demonstrate their awareness and have an understanding of their responsibilities.	Medium
There are processes in place to ensure information risks are managed throughout the organisation in a structured way.	A.03. LCC have a SIRO and Information Asset Owners (IAO) in place. However, appropriate responsibility for information risk management has not been assigned consistently across LCC. Although IAOs have recently attended IAO awareness sessions and an IAO awareness	A.03. LCC must ensure that all IAOs are made aware of their responsibility for information risk management. Furthermore, LCC must either develop their information risk information within their current risk policy or create a stand-alone information	Medium

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	handbook is made available to them, it was identified during interviews that IAOs are not fully aware of their responsibilities. In addition to this, LCC have a Risk management policy and strategy in place which touches on information risk but does not provide enough detail. If information risk management is not effective, LCC cannot be sure they are preventing misuse of personal data. This may result in a personal data breach, or risk of non-compliance with UK GDPR Article 5(f), 5(2), 32, and/ or DPA 2018 sections 34(3), 40, and 66.	risk policy or procedure which is subject to senior management approval, that undergoes periodic reviews. The information risk policy must be communicated effectively to staff so that they are fully aware of the contents. This will ensure that processes are in place to ensure that information risks are assessed, documented, and controlled effectively in all areas of LCC.	
There is an Information Management Steering Group, Committee, or equivalent, in place, which is responsible for providing the general oversight for information governance and data protection compliance activity within the organisation.	A.04. LCC used to have three IG specific groups in place that met on a regular basis. However, because of restructure this is being made into one information management steering group. It was reported that the plan for this group is to meet every two months to have oversight of IG and DP compliance. The draft (ToR) for the information management group was provided to ICO auditors but at the time of audit, the first meeting had not yet happened. Without an information steering group in place, there may be a lack of coordination between different areas of LCC. Strategic level management may be misinformed or misled, resulting in breaches. This risks non-conformance with UK GDPR Article 5(2) and 39.	A.04. LCC must continue with their plans for their newly restructured information management group, ensuring that meetings happen regularly as stated within the draft ToR provided. The steering group should have oversight of a full range of DP related topics including DP key performance indicators (KPIs), issues and risks. LCC must ensure that the group is chaired by an appropriately senior role with the DPO effectively involved in the group. This will ensure that LCC have oversight of a full range of data protection related topics including any issues and risks.	Medium
Management support and direction for data protection compliance is	A.05. LCC have some policies in place such as a DP policy, Records management (RM) policy and Information assurance (IA) policy but they	A.05. LCC must continue with their plans to review, update and create any missing DP/IG policies and procedures. These	Urgent

Page 87

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
set out in a framework of policies and procedures.	have not been reviewed regularly and contain some out of date information. In addition to this, LCC do not have some policies and operational procedures in place such as a Data sharing policy, or a documented procedure for requests for information received from the police. Without formalised and documented policies and procedures in place, LCC risks policies being miscommunicated when passed on verbally. Staff may also be unsure of correct procedure, but have no reference material or guidance to check. Breaches may occur because of incorrect assumptions by staff. Operational staff may not be clear on data protection and organisational requirements, which can lead to a data breach. This may result in non-conformance with UK GDPR Article 5(2) and DPA 2018 sections 34(3) and 71(2).	documents should be suitably extensive for the context of LCC and provide staff with sufficient direction that they are able to identify their roles and responsibilities. In addition, all policies should be reviewed in line with review dates and kept up to date and fit for purpose. All policies, procedures and guidelines must display document control information, as a minimum this should include the version number, owner, review date and change history. The review and approval process should be sufficient in the context of LCC to provide assurance of the effectiveness of the policies and procedures. This will help ensure consistent practice across LCC and compliance with UK GDPR Article 5(2) and DPA 2018 sections 34(3) and 71(2). Further guidance on policies and procedures can be found on the ICO website.	
Policies and procedures are approved by senior management and subject to routine review to ensure they remain fit-for-purpose.	A.06. ICO auditors did not gain assurance that LCC have a documented process in place for reviewing, ratifying and approving all new and existing policies and procedures. Some policies do not contain document control information and are not signed off by an appropriate senior member of staff. Documents containing outdated information or	See A.05	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	giving incorrect directions could cause breaches. Staff may also be unable to tell whether a document is up to date or an older version. This may lead to no ownership of policy and procedures and non-conformance with UK GDPR Article 5(2).		
Policies and procedures are readily available to staff and are communicated through various channels to maintain staff awareness	A.07. Policies and procedures are made available to staff on LCC's intranet site. However, some LCC staff such as cleaners do not have access to LCC systems. This means that they may not have access to the DP policies in place, unless these are made available to them in another format. In addition, although updated policies are communicated to staff, LCC are unable to guarantee whether or not staff read DP/IG policies that are circulated by email or added to the intranet. If policies are not read, breaches may be caused by staff being unaware of their responsibilities. This can lead to risks being uncontrolled as staff act without reference to guidance. There may be a non-conformance with UK GDPR Articles 5(1) and 5(2).	A.07. LCC must ensure that new and updated policies are read and understood by all staff. LCC must implement a method by which they are able to gain assurance that all staff are reading policies, for instance, signing a form that is refreshed on a periodic basis stating that IG policies have been read. Furthermore, LCC must make relevant DP/IG policies available to staff that don't have access to LCC systems. This will help LCC gain assurance that all staff are fully aware of the contents of policies and procedures that are relevant to their role and that staff know where to find them.	High
There is an overarching IG training programme in place for all staff.	A.08. LCC have an IG training programme in place. There is corporate wide Level 1 IG online training that is made available to all staff that have access to LCC systems. This training is completed at induction stage and refreshed every two years. The training includes seven modules, with the module at the end being a quiz with seven questions to test staff	A.08. LCC must continue with their plans to provide access to the online IG training to all staff that work for the council including temporary and agency staff. If some staff are still unable to access the online training, LCC must complete a training needs analysis (TNA) to assess where additional training may be required around specific	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	knowledge. However, the pass mark for this is a minimum of four correct answers, which may mean some staff have gaps in knowledge even if they pass the quiz. Staff with no access to LCC systems are provided with a DP brochure and a letter from the SIRO. Their manager would then sign off on the system stating that they have completed the training. This means that staff with no access to the online training may not be getting the same amount of training, and assurance cannot be provided that they are definitely reading the brochure provided to them. If staff do not receive adequate DP training, they may be unaware of or unable to properly carry out their responsibilities, causing breaches. This may result in non-conformance with UK GDPR Articles 5(1) and 5(2).	topics or for specific roles. LCC must also review the current IG training they have on offer, ensuring that it is up to date and includes appropriate testing with a more suitable pass mark at the quiz stage. Once updated, it should be circulated to all staff to complete, and a record must be kept of training completion rates. LCC should continue to refresh this training on a periodic basis appropriate to the context of the council. This will help LCC gain assurance that all staff are fully trained in all relevant aspects of IG.	
Induction training is in place and delivered in a timely manner to all staff including temporary and agency staff etc.	See A.08	See A.08	
Refresher training is in place and delivered in a timely manner to all staff including temporary and agency staff etc.	See A.08	See A.08	
There is provision of more specific DP training for specialised roles (such as the DPO, SIRO, IAOs)	A.09. Some additional DP training is available for staff within LCC who have responsibilities which require more extensive data protection knowledge, for example, the SIRO, deputy	A.09. Once a TNA is completed, LCC must ensure specific DP training is completed by staff in specialised key roles within the council. This training should be mandatory,	High

Page 90

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
or particular functions e.g. records management teams, SAR teams, information security teams etc.	SIRO and some IG staff. However, not all staff with specialised roles receive more specific training. It was noted during interviews that some staff that have specialised key roles are only expected to complete Level 1 IG training. Specialised training is available, however it is the responsibility of service managers to request this for the staff they manage. DP training may not be a priority in all service areas, which could lead to DP training needs not being met. Furthermore, no TNA has been carried out recently to identify staff who may require additional training. If specific data protection training is not provided, breaches may be caused by lack of specialist knowledge. This risks non-conformance with Article 5(1) of the UK GDPR.	specific to the responsibilities of the individual and subject to refresher training on a regular basis. This would ensure that specialised roles with DP responsibilities receive additional training beyond the basic provided to all staff.	
The organisation has considered a programme of external audit with a view to enhancing the control environment in place around data handling and information assurance	A.10. ICO auditors were provided with a copy of the Grant Thornton's IT audit findings. Although these findings are from their IT systems and applications, they still relate to DP. However, LCC do not have a programme of external audits in place specifically for IG and DP. A reliance on internal audits and assurances can result in blind spots, causing inaccurate risk assessment and potential breaches. This risks non- conformance with UK GDPR Article 5(1).	A.10. LCC should consider employing the services of an external audit provider to provide independent assurances on compliance with DP legislation and information security for the whole council and not just for IT systems and applications. The DPO would need to have oversight and input into the external audit programme. This will ensure that LCC is carrying out external audit procedures to provide independent assurances of the effectiveness of the council's controls.	Medium

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
There is a programme of risk- based internal audit in place covering information governance / data protection.	A.11. LCC have a risk based internal audit plan in place which includes auditing some DP/IG aspects; however, there is currently no specific DP/IG audit programme. It was reported at interviews that DP/IG audits are currently done on an ad-hoc basis. Without a documented DP audit programme in place, LCC has no assurance that their risk management is sufficient or effective, this risks non-conformance with UK GDPR Article 5(1).	A.11. LCC should create an internal audit programme specific to DP with oversight and input from the DPO. LCC should then carry out regular internal DP and IG audits, sufficiently detailed for the context of LCC. Audit reports should be produced to document the findings and a central action plan should be in place to take forward the outputs from the audits. By implementing internal DP audits, LCC can gain assurance that their risk management is effective and guarantees compliance with UK GDPR Article 5(1). The ICO's Accountability Framework may help LCC to establish a plan for these audits.	High
The organisation actively monitors or audits its own compliance with the requirements set out in its data protection policies and procedures.	A.12. LCC conduct some compliance checks, such as monthly manager checks on case notes within some services. However, ICO auditors did not gain assurance that compliance checks are done on a regular basis across LCC. Furthermore LCC's DP policies and procedures do not clearly set out how compliance with the policy or procedure will be monitored. Without ongoing compliance monitoring, controls gradually stop being implemented or may be incorrectly implemented, potentially leading to breaches. This risks non-conformance with UK GDPR Articles 5 (1) and 5(2).	A.12. LCC must conduct routine compliance checks to test staff compliance with DP policies and procedures. They must also ensure that their compliance checks are formalised and documented. In addition, they should update their DP policies and procedures to set out how compliance with the policy or procedure will be monitored. This will ensure that LCC has documented how it will monitor adherence to requirements set out in its own policies and procedures and then ensures compliance to these requirements through physical routine compliance monitoring.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are data protection Key Performance Indicators (KPI) in place	A.13. LCC have some DP KPIs in place, such as KPIs for responding to SARs and FOI/EIR requests. However, they do not have all DP KPIs in place, for example there are no KPIs in place for records management. It was reported during interviews that LCC are currently working on a suite of DP KPIs but have not gone live with them yet. The DP KPIs LCC have in place are included in an annual IG report which is made available to senior management. However, as the suite of DP KPIs has not gone live yet, ICO auditors did not gain assurance that KPIs are reviewed regularly at IG operational team meetings or that there is a dashboard in place giving a high level summary of performance in all key IG related KPIs. KPIs provide a valuable tool for oversight to understand the effectiveness of control measures. Without gathering these, risks may be inaccurately assessed and managed, leading to breaches. This may result in non-conformance with UK GDPR Article 5(2).	A.13. LCC must continue with their plans to implement DP KPIs that are proportionate to the size of the council. LCC should ensure they have a dashboard in place that gives a high level summary of performance in all key IG related KPIs. KPI performance should be reported to and reviewed regularly in appropriate operational and leadership meetings. This will confirm that all gathered KPI management information is clearly being communicated to relevant stakeholders, and is informing their subsequent discussions, decisions, and actions.	Medium
Performance to IG KPIs is reported and reviewed regularly.	See A.13	See A.13	
There are written contracts in place with every processor acting on behalf of the organisation which set out the details of the processing	A.14. LCC have written contracts in place with processors acting on behalf of the council and have a procurement calendar that documents all of the contracts they have in place (both processor and controller contracts). The services at LCC that require processor contracts to be put in place are responsible for contract management. This includes keeping a log of all	A.14. LCC should conduct periodic compliance checks on the processor contracts they have in place. These checks should help LCC ensure that the different services are keeping a centralised log of all the processor contracts they have in place, and are reviewing them on a regular basis to ensure they remain up to date. This will	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
	the processor contracts the service has in place and ensuring contracts are reviewed on a periodic basis and remain up to date. No compliance checks are conducted by the IG team on the processor contracts in place, so LCC cannot guarantee that contracts are being managed correctly by the different services within the council. If processor contracts are not reviewed regularly or managed correctly, LCC may not understand how personal data is being processed by third parties, there may be a breach of controller/processor requirements and may be in non-conformance with UK GDPR Articles 28 and 5 (2).	help LCC gain assurance that staff understand how personal data is being processed by third parties and be in conformance with UK GDPR Articles 28 and 5 (2).	
The organisation takes accountability for ensuring all processors comply with the terms of the written contract(s)	A.15. Clauses are included within contracts that allow LCC to conduct audits or checks to confirm the processor is complying with all contract terms and conditions. However LCC could not provide assurance that any audits or checks are conducted to test that processors are complying with contractual agreements. If no compliance activities are carried out, LCC has no assurance that their processors are actually abiding by the terms of their contract, which can lead to a potential risk of breach, and non-conformance with UK GDPR Articles 28 and 5(2).	A.15. LCC must ensure that routine audits or compliance checks are conducted to ensure processors are complying with all contract terms and conditions. The checks should be proportionate and appropriate for the risk of processing undertaken. This will help LCC guarantee that they use the opportunity to review the compliance of processors with their contracts.	Urgent
The organisation has a process to ensure all processing activities are	A.16. LCC could not confirm when their last information audit or data mapping exercise was conducted to find out what personal data the	A.16. LCC must complete an information audit to find out what personal data they hold. LCC should consult staff across the	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
documented accurately and effectively	council holds. Without a clear understanding of their processing activities, further activities such as development of a record of processing activities (ROPA), information asset registers (IAR), and risk assessments may be based on inaccurate or incomplete information, which could infringe on their compliance with UK GDPR Article 30.	council to get a more complete picture of their processing activities, for example by using questionnaires or staff surveys. Carrying out comprehensive information audits or data mapping exercises will give LCC a clear understanding of their information processing.	
There is an internal record of all processing activities undertaken by the organisation	A.17. LCC have a library for all council records of ROPA. There is a ROPA in place for each service, for example, a safeguarding ROPA. The ROPAs LCC have in place were created when GDPR was introduced, with responsibility being assigned to IAOs to review and maintain the ROPA for their specific service. However, the ROPAs are all out of date, have not been reviewed regularly and do not contain everything they should, for instance, there is no lawful basis or retention information. It was reported during interviews that LCC are currently developing their IAR and plan to imbed the ROPA within it. Without an adequate ROPA in place, LCC may be in breach of UK GDPR requirements. If the ROPA does not have its foundation in a data mapping exercise, it may not be complete or accurate, which could infringe on their compliance with UK GDPR Article 30.	A.17. After completing a comprehensive information audit, LCC must continue with their plans to have a centralised log of all processing activities and create a centralised ROPA document. As a minimum the record should include: - The name and contact details of the council (and where applicable, of other controllers, their representative and the data protection officer); - The purposes of the processing; - A description of the categories of individuals and categories of personal data; - The categories of recipients of personal data; - Retention schedules; - A description of the technical and organisational security measures in place. The processing activities should be documented in electronic form so information can be added, removed and amended easily. LCC should put a process in place to ensure the record is reviewed on a regular basis to maintain accuracy with	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
		current processing activities, policies and procedures. The record of processing goes further than minimum requirements. LCC must ensure that the ROPA contains all relevant requirements from the legislation. Further information about ROPA and what it should include can be found on the ICO website.	
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UKGDPR	See A.17	See A.17	
Consents are regularly reviewed to check that the relationship, the processing and the purposes have not changed and there are processes in place to refresh consent at appropriate intervals.	A.18. It was reported during interviews that LCC have an expectation for consents to be reviewed regularly. However, the service at the council that obtained consent are responsible for these reviews. This means that reviews may not be done regularly or in a uniform manner across the council. There is no centralised log for all records of consent as each service is supposed to maintain their own log of consents. In addition, no spot checks are conducted on records of consents to ensure they are being recorded correctly and reviewed regularly. If consent is not regularly reviewed, the nature of the processing may change sufficiently to no longer be what was consented to. This could place the council in breach of UK GDPR Articles 6 and 9.	A.18. LCC must ensure that there is a documented process put in place to review consents and check that the relationship, the processing and the purposes have not changed. In addition to this, a documented process must be in place to refresh consent at appropriate intervals. These processes should be shared with all relevant LCC staff. Spot checks by the IG team should then be conducted to gain assurance that staff are complying with the consents review process. This will help LCC guarantee that there are proactive reviews of previously gathered consent, which demonstrate an honest commitment to confirming and refreshing the consents.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Where the lawful basis is Legal Obligation, the organisation has clearly documented the obligation under law for that type of processing activity for transparency purposes.	A.19. Legal obligation is clearly detailed in LCC's privacy information. However, individuals are not always informed which data subject rights would not apply to their personal data processed under this basis. If LCC does not have this decision clearly documented, they may be in breach of UK GDPR Articles 5 (2) and 6.	A.19. LCC must ensure that where the lawful basis is legal obligation, individuals are informed of which data subject rights would not apply to their personal data processed under this basis and clearly communicate this to individuals. LCC should also hold a documented, honest analysis of whether their legal obligation is the appropriate lawful basis. This will help LCC be compliant with UK GDPR Articles 5 (2) and 6.	High
The organisations privacy information or notice includes all the information as required under Articles 13 & 14 of the UKGDPR.	A.20. LCC have a main privacy notice in place and several other privacy notices for specific services such as the benefits privacy notice and a council housing privacy notice. The notices contain information required under Articles 13 & 14 of the UK GDPR such as contact details for the DPO and purposes of processing. However, they do not all include all required information, for instance retention periods for the personal data. If the basic requirements are not met, then data subjects cannot have been properly informed of how their information is being processed.	A.20. LCC must continue with their plans to conduct a review of all of their privacy notices, so that they include all the information required under Articles 13 & 14 of the UK GDPR. This will ensure that privacy information is sufficient to meet the legal requirements. Further details on privacy information can be found on the ICO website.	Urgent
Existing privacy information is regularly reviewed and, where necessary, updated appropriately.	A.21. LCC do not have a centralised log for all their privacy notices, nor do they keep a record of when they were last reviewed. In addition to this, a log of historical privacy notices is not maintained. During the audit, ICO auditors identified a number of LCC privacy notices that have not been reviewed regularly. Currently, it is the responsibility of staff from the different	See A.20 A.21. LCC must ensure that privacy information is reviewed against the ROPA, once established, to ensure that it remains up to date and explains what happens with individuals' personal data. They must also maintain a log of historical privacy notices	Urgent

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	services across the council to review the notices, or inform the IG team when these need to be reviewed. It was reported at interview stage that some services make contact with the IG team more regularly than others. Furthermore, LCC do not carry out user testing to evaluate how effective their privacy information is. If privacy information is out of date, data subjects are not being properly informed of their rights and how their information is being processed. If there is no check on the effectiveness of the communication of privacy information, LCC has no assurance that data subjects are actually receiving the privacy information.	including the dates on which any changes were made, in order to allow a review of what privacy information was provided to data subjects on what date. If there are plans to use personal data for a new purpose, LCC should ensure that there is a process in place to update the privacy information and communicate the changes to individuals before starting any new processing. LCC should carry out user testing to evaluate how effective their privacy information is. This will confirm that LCC has carried out a pattern of effective reviews which update both the contents of the privacy information, and how it is communicated.	
Fair processing policies and privacy information are understood by all staff and there is periodic training provided to front line staff whose role includes the collection of personal data on a regular basis.	A.22. It was reported during interviews that some frontline staff, such as contact centre staff, receive specialised fair processing and privacy information training. However, ICO auditors did not gain assurance that this was in place for all front line staff whose role includes the collection of personal data. If front line staff are untrained on privacy information, individuals may be misdirected or given incorrect information which means LCC is at risk of a breach of UK GDPR.	A.22. LCC must ensure that all front line staff whose role includes the collection of personal data complete specialised fair processing and privacy information training on a periodic basis. This will ensure that LCC can demonstrate that their front line staff are able to explain the necessary privacy information, and provide guidance to any individual with queries. These staff should have received training to this effect.	Medium
The organisation proactively takes steps to ensure that through the lifecycle of the processing activities they only	A.23. LCC do not have a centralised ROPA. This means that LCC have no way of guaranteeing that they only process, share and store data they need in order to provide their services.	See A.17. A.23. LCC must create internal policies which outline their approach to data minimisation and pseudonymisation.	High

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
process, share and store the data they need in order to provide their products or services.	Furthermore, ICO auditors did not gain assurance that LCC have internal policies and measures in place which outline LCC's approach to data minimisation and pseudonymisation. In addition to this, retained data is not always reviewed on a regular basis to identify opportunities for pseudonymisation and minimisation. This risks non-compliance with UK GDPR Articles 5(b/c/e), 35, and 25(2).	Retained data must be reviewed on a regular basis to identify opportunities for pseudonymisation and minimisation, which should be documented in the retention schedule. This will confirm that LCC ensures they process the least information possible and information is not retained longer than necessary. It also ensures that LCC has considered and implemented appropriate data minimisation procedures.	
Existing policies, processes and procedures include references to DPIA requirements	A.24. LCC's DP policy includes reference to Data Protection Impact Assessments (DPIA) requirements. However, as the DP policy has not been reviewed since 2018 it does not include up to date DPIA information. Furthermore, not all main project and change management policies and procedures reference DPIA requirements. If DPIA requirements are not built in at the ground level, then the requirement of privacy by design and default is not likely to be met. This risks non-conformance with UK GDPR Article 35.	A.24. LCC must ensure that they review and update the DPIA requirements set out in the DP policy. In addition to this, all main project and change management policies and procedures should also include DPIA requirements. This would help LCC gain assurance that DPIAs have been built into the basic governance framework of the council.	High
The organisation understands the types of processing that requires a DPIA, and uses a screening checklist to identify the need for a DPIA, where necessary.	A.25. It was reported during interviews that currently, staff are expected to complete a DPIA before processing of any personal data takes place, however this is not always the case. LCC's DPIA template has six screening questions that should be completed before a DPIA is conducted. However, the screening	A.25. LCC must continue with their plans of implementing a screening checklist on their DPIA power app. The screening checklist should include all the relevant considerations on the scope, type and manner of the proposed processing. Where the screening checklist indicates a DPIA is not required, documented evidence should	High

Governance & Accountability

Control	Non-conformity	Recommendation	Priority
	questions are not sufficient enough to properly assess whether a DPIA should be completed. To address this, LCC are developing a DPIA power app that will include a DPIA screening checklist to aid staff in determining whether a DPIA is required. Without a sufficient DPIA screening checklist, understanding may not be in place of when a DPIA should be conducted. LCC may be conducting DPIAs where they are not required.	be retained of this decision. This will ensure that understanding is clearly demonstrated, both on a procedural level and by the relevant staff.	
DPIAs are undertaken before carrying out types of processing likely to result in high risk to individuals' rights and freedoms and meet the requirements as set out in Article 35 of the UKGDPR.	A.26. LCC have DPIA training and a DPIA flow chart in place to help staff complete DPIAs. However, they do not have a documented process in place that provides further detail that is not available in the DPIA flow chart. If there is no documented DPIA process, the process which gets followed may not be sufficient on each occasion to meet the requirements of UK GDPR Article 35 and 39.	A.26. LCC must create a documented DPIA process that is read in conjunction with the DPIA flow chart. LCC must ensure the DPIA process includes appropriate document controls and is reviewed periodically to ensure it remains up to date. In addition to this, the process should include; an objective assessment of the likelihood and severity of any risks to individuals' rights and interests; a check that the processing is necessary for and proportionate to the purposes and consultation with any data processors to help understand and document their processing activities and identify any associated risks. This will help LCC confirm that the DPIA process is documented, comprehensive, and has been approved by mechanisms appropriate to the context of the council. Further information on DPIAs, including guidance of when you need a DPIA, how to	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
		carry out a DPIA and a sample DPIA template can be found on the ICO website.	
	A.27. LCC make staff aware that DPIAs must be conducted before carrying out all types of processing of personal data, with a DPIA template made available to them on the intranet. However, it was reported during interviews that in the past DPIAs have not always been carried out where they should have been. In addition to this, LCC do not have a centralised log of all DPIAs they have in place. ICO auditors were provided with a DPIA internal audit follow up report, which also identified that DPIAs were not carried out in all instances as expected. However, the report highlighted that this is now improving. If DPIAs are not carried out before high risk processing then LCC will be in breach of UK GDPR.	A.27. LCC must continue with their plans to implement the DPIA power app. This app should help LCC have a centralised log of all DPIAs and ensure that DPIAs are always completed before carrying out types of processing likely to result in high risk to individuals' rights and freedoms. This will ensure that LCC can demonstrate that DPIAs are carried out in advance of such processing, and that all DPIAs are done to the documented and required standard.	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is an RM policy framework in place, which is subject to senior management approval and periodic reviews to ensure it aligns with the latest guidelines	B.01. The records management policy provides an overview of records management but does not provide sufficient detail to staff. LCC is aware that the policy review date has expired, and the document will reportedly be reviewed as part of the Information Governance (IG) work plan.	See A.05 B.01. Review and implement an appropriate records management policy. The policy should set out how information assets are recorded and risk assessed, how information is stored and where retention periods are documented, how information is	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
	If records management requirements are not fully documented, it may lead to inconsistent approaches to records management within LCC, and may infringe on Article 5(2) of the UK GDPR.	kept secure and how access permissions are managed. The policy should be subject to senior management approval and periodic reviews to ensure that it remains fit for purpose. The ICO has produced guidance on records management which includes an extensive 'Further reading' section listing helpful resources from The National Archives.	
RM is incorporated within a formal training programme and good records management practices are promoted across the organisation	See A.08 B.02.a. The IG level 1 training includes some record management requirements and examples of how records management should be applied in day to day roles within LCC. However the training does not provide sufficient detail around the records management policy and standards of LCC. B.02.b. The percentage of questions that need to be answered correctly to pass the IG level 1 training is approximately 57%. ICO auditors do not consider this pass mark to offer adequate assurance that staff know and understand their IG and records management obligations. Furthermore, due to the number of questions asked as part of the assessment, and the size of the question bank used to test staffs' understanding, staff may only be asked a very limited number of questions relating to records management.	See A.08 B.02.a. Ensure that IG training adequately covers record management requirements. The content of the training should link to the records management policy framework to enhance compliance with associated policies and procedures. See recommendation B.01. This will ensure that all staff are aware of their obligations with respect to records management and are competent to carry them out.	Medium
The process for the creation of records or	B.03. ICO auditors do not have assurance that there is a cohesive approach and sufficient	B.03. Ensure detailed procedures for creating records or developing documented	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
development of documented information is formalised and controlled	oversight of the creation of records throughout the Council. Not all documents, such as policies and procedures, record change history or effectively apply version controls. It was also unclear whether the IG Records Manager Lead had approved all policies or procedures relating to records management because the change history is not consistently recorded on documents. If the creation of new records or development of documented information is not formalised and controlled, the Council risks that uncontrolled, inaccurate versions may exist, be inappropriately communicated, and may confuse staff. This may result in a breach of Articles 5(1)(d, e, f), 5(2), and 32 of the UK GDPR.	information are effectively implemented throughout the Council. LCC should ensure that all documented information is subject to standardised formatting procedures, a record of approval is maintained, and sufficient change/version controls are used to achieve a consistent approach, so that inaccurate versions cannot be accessed by staff. The procedures should be communicated to all staff, controlled, and monitored to promote adherence. This will help LCC to comply with the UK GDPR.	
When creating records and documented information the organisation has ensured there are appropriate identification and classification measures applied	B.04. LCC does not have an organisation wide identification and classification scheme, however it is in the process of implementing one. If there is no identification and classification scheme in use, LCC risks that records or documented information may spread to inappropriate users, or may not clearly be designated in terms of what it contains, who should use it, or where it should be, potentially resulting in a personal data breach or a breach Articles 5(1)(f) and 32 of UK GDPR.	B.04. Ensure procedures are in place across the Council for the appropriate identification and classification of all records/information, and that checks are undertaken to confirm that those procedures are being followed. This will ensure documents are appropriately protected and sharing is restricted in line with the classification requirements. This will help LCC clearly identify and classify records appropriately and comply with the UK GDPR.	High
There has been an information audit carried out across the organisation	See A.16 B.05. LCC is laying the groundwork so they can	See A.16 B.05. Complete an information audit to	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
to identify the data processed, and how it flows into, through, and out of the organisation	complete a comprehensive information audit across the Council. IAOs have recently completed the relevant training, and the content of the IAR is under review to ensure it contains all applicable information. Until LCC has carried out a full information audit, there is a risk that personal data may be being processed without organisational awareness, and that information assets may not have been identified, properly risk-assessed or have the appropriate controls implemented. This may result in non-compliance with Articles 5(1)(f), 5(2), and 32 of UK GDPR.	identify information assets across the Council. The results of the audit should be regularly reviewed to ensure they remain accurate. The National Archives has produced guidance on Identifying Information Assets and Business Requirements which will help with this process.	
A comprehensive inventory or asset register is in place and maintained that shows what records are held, what they contain, in what format, and what value they have for the organisation	B.06. LCC's current IAR template does not record all the relevant details of each information asset. In addition, several IARs are incomplete with gaps/blank entries where details have not been completed. Without an up to date IAR, LCC will not be able to demonstrate that they have identified and risk-assessed the information they hold, which risks non-compliance with Article 5(2) of the UK GDPR.	B.06. Ensure the IAR template records the name of the asset, a brief description, the location of the asset, the IAO, the volume of information, and details of associated security measures. Each asset should also be risk-assessed, so that high-risk assets can be identified and addressed as necessary. The IAR should record the information assets identified by the information audit. The IAR should be periodically reviewed, with particular reference given to risk-assessment scores to ensure that these remain reflective of the current risk associated with each asset.	High
Appropriate access controls are in place to mitigate the risk of unauthorised access to physical records	B.07. There are security measures in place at the LCC offices and records storage facilities, however some security measures were inadequate. For example, keys for locks were lost or missing and push button coded door locks had not had their codes regularly	B.07. Ensure that areas where physical records are stored in-house, have appropriate access controls to mitigate the risk of unauthorised access. This will help to ensure that personal data stored in physical records is not inappropriately accessed.	High

Records Management

Control	Non-conformity	Recommendation	Priority
	changed. Without appropriate access controls in place, there is a risk of unauthorised access and of a subsequent data breach.		
Periodic audits are carried out to assure the security of 'in-house' records storage	B.08. LCC does not carry out periodic audits or checks on the security of 'in-house' records storage but will review security measures following a security breach or near miss. This means that threats to, or breaches of security may not be identified in a timely manner. This poses a security risk under Articles 5(1)(f) and 32 of the UK GDPR, and further risks that any resultant personal data breaches are not reported where required by Article 33 of the UK GDPR.	See A.11 B.08. Ensure appropriate resource is designated to carry out periodic checks on the security of 'in-house' records storage across the Council, to ensure that LCC's record storage is appropriately secure.	High
Where semi-current paper based records are stored by a contractor the organisation has established the right to periodically visit their premises.	B.09. LCC have not exercised their right to visit the premises of Restore, the provider of the semi-current paper based records store, but an audit is planned for January 2024. Without assurance of security, LCC risks that documents may be accessed inappropriately, which may result in a breach of Articles 5(1)(f) and 32 of UK GDPR.	B.09. Conduct the planned audit of Restore to ensure that the records storage facility is appropriately secure to minimise the risk to the personal data stored there.	Medium
There is a policy that documents the arrangements for the access and security of electronic records in line with accepted standards and good practice.	B.10. LCC has several policies and protocols which refer to access controls and security arrangements of electronic records, however they do not amount to a complete and clearly documented policy. Furthermore, many of the policies and protocols are inaccurate and/or overdue for review.	B.10. Create a policy which sets out the arrangements for the access to, and security of electronic records. The policy should include details on how access permissions for staff members will be determined, implemented, monitored and maintained, as well as details of the	Medium

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
	For example, the Acceptable Use Protocol is overdue a review and is no longer fit for purpose as the drives referred to in the protocol, have been copied to SharePoint. Having inaccurate protocols and multiple storage locations for the same information could result in staff, especially staff that have moved roles in LCC, having inappropriate access to personal data. Although staff members' access permissions are associated with their role, and requests for further access are always carefully considered, the lack of an accurate and clearly documented policy may result in inconsistencies between access permissions or even inappropriate access. This risks a contravention of Article 5(1)(f) of the UK GDPR.	technical measures in place to keep electronic records secure.	
Appropriate access controls are in place to mitigate the risk of unauthorised access to electronic records	B.11. ICO auditors were unable to gain assurance that access to electronic records containing personal data is reviewed and monitored in a standardised and controlled way. Whilst some interviewees described how this might be achieved for specific electronic records, there is no formalised, standardised approach outlined in an overarching policy, so it is not consistently completed, and requirements and timescales vary. There is a risk that records could be accessed without the necessary authority. Without appropriate controls in place, the organisation risks unauthorised access to personal data	B.11. Ensure that access to electronic records containing personal data is regularly reviewed and monitored in a standardised and controlled way, to ensure that unauthorised individuals are unable to access personal data stored electronically.	Medium

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
	taking place. This may breach Articles 5 (1)(f) and 32 of the UK GDPR.		
The whereabouts of records are known at all times and the movement of records between storage and office areas is logged and tracked to facilitate control and provide an audit trail of all record transactions	B.12. It was reported to ICO auditors that entries on the physical records log do not always accurately reflect the record stored. For example, when ICO auditors tested whether a record matched the records log, it was found that the record had been logged as 'adult social care' when it should have been logged as 'finance'. If physical record logs are inaccurate, then the Council cannot reliably track the movement or location of the record and there is a risk that personal data may be lost or misplaced. This may result in a breach of data protection legislation.	B.12. Continue the process of identifying inaccurate historic physical records and ensure that record logs are amended accordingly. Take measures to ensure that future physical record logs are accurate, so records can be tracked and retrieved where necessary.	Medium
The security of manual and electronic records transferred within the organisation and externally to any third party is maintained	B.13.a. ICO auditors were advised that the 'How to supply viewings' and 'Viewing LCC (External and Police Viewing with file request) guidance documents were created during the Covid period and no longer reflect current practices. If procedures are inaccurate, then different and incorrect practices may take place across the Council, which could risk the security of manual and electronic records. B.13.b. Computer logins and passwords are included in the guidance documents, which is widely accessible within LCC. Furthermore, the passwords are not complex and would not be considered 'strong', nor are they regularly changed. This does not represent good practice with respect to access control and represents a	B.13.a and B.13.b. Review current guidance documents to ensure they meet data protection requirements, are accurate and reflect current practices. The guidance should then be subject to periodic reviews to ensure it remains fit for purpose. Passwords should be secure, strong and be kept confidential, to reduce security risks and the risk of unauthorised or unlawful access to personal data. B.13.c. Ensure personal data is transferred securely, using appropriate organisation and technical measures. Undertaking a DPIA for data sharing operations and implementing information sharing agreements can be an effective means of	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
	risk of non-compliance with Article 5(1)(f) and Article 32 of the UK GDPR. B.13.c. The policy around non-LCC staff and Police taking notes and copies of records was inconsistently reported to ICO auditors. Whilst note taking may be practical, it introduces additional risks, for example data being inaccurately noted and security risks if a note containing personal identifiable data is lost or stolen; a note could be easier to lose and harder to trace and report. The time of transfer is a point of weakness, where security is more difficult to ensure. If the LCC does not maintain good security, the risk inappropriate access, loss, and personal data breach. May breach Articles 5(1)(f) and 32. See non-conformity B.07 regarding the physical security controls in place to protect the external transfer of manual data/paper record by post via the post room.	considering these issues and implementing appropriate mitigation measures. The process of transferring information, some of which may be sensitive, outside of the Council poses a risk to LCC, and whilst the sharing of information is vital, it should be done in a way that minimises the risk of a personal data breach and of non-compliance with UK GDPR. Also see recommendation B.07.	
There are procedures in place which allow individuals to challenge the accuracy of the information the organisation holds about them and have it corrected if necessary. Where the inaccuracies are unable to be rectified procedures	B.14.a. Individuals are not advised of their individual rights within LCC's privacy notice, which is a key transparency requirement under the UK GDPR. If this basic requirement is not met, then individuals have not been properly informed of their individual rights in respect of the processing of their personal data, which is required under Articles 13 and 14 of the UK GPDR. The transparency requirements under Article 12 of UK GDPR are also not being met.	See A.20 B.14.a. Review the LCC privacy information or notice to ensure it advises individuals of their rights and is sufficient to meet the legal requirements under UK GDPR. B.14.b. Ensure that LCC's data subjects are fully informed of their individual rights and how they can make a request.	Urgent

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
dictate that the inaccuracy is documented	B.14.b. An individual can make a request to exercise the individual rights verbally or in writing, however, the LCC website does not explain that individuals have a choice and does not provide any details on how an individual can make a request by telephone or post. Furthermore, the website requires the individual to upload an identity document (ID), which requires the individual to be IT literate. The individual may not want to upload a copy of their ID through the website, so alternative methods of providing proof of ID should also be explained. If individuals are not given sufficient guidance, they may not be aware of their rights. Furthermore, they may make requests in such a fashion that LCC is unable to respond effectively. This may result in a breach of Articles 12 of UK GDPR. B.14.c. LCC staff were able to explain the individual rights operational processes, and screenshots were provided which confirmed there is guidance available to staff. However, no policies or procedures were seen by ICO auditors that instruct or advise operational staff on how to handle individual rights requests. If there are no documented policies and procedures the organisation may not handle requests according to agreed processes, may handle requests inefficiently, or may fail to meet their statutory requirements, which may result in a breach of data protection legislation.	B.14.c. Create a formal procedure for handling requests made under individual rights. The procedure should set out where data is inaccurate according to data protection law, what steps should be taken to correct inaccurate data, and how to provide a response to the requester. It should also cover what action should be taken where the data disputed is not necessarily inaccurate, and how to provide a response to the requester in this case. The ICO has produced guidance on the right to rectification.	
Where inaccuracies in data that is shared with 3rd	B.15.a. LCC operational staff have no reliable way of identifying whether personal data has	B.15.a and B.15.c. Implement a formal process for recording and identifying where	High

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
parties has been identified, there are procedures in place to ensure the 3rd party is informed in a timely manner	been shared with a third party. If staff are unable to reliably identify if personal data has been shared and who that third party is, then the Council risk breaching their legal obligations regarding the accuracy of personal data. B.15.b. LCC's information sharing agreements do not provide sufficient detail or direction to both parties to ensure that the requirements of data protection legislation regarding the accuracy of data is met, which could result in a breach of data protection regulations. B.15.c. As explained within non-conformity B.14.c, the process for assessing and dealing with rectification requests, including the process for identifying whether personal data has been shared with a third party, is not formally documented within a policy and/or procedure. If this process is not formally documented, there is a risk that a rectification request will not be dealt with appropriately and may result in a breach of Article 5 (1)(d) of UK GDPR.	personal data has been shared with a third party. Please refer to recommendation B.14.c. regarding the creation of a formal procedure for handling individual rights requests. The policy and/or procedure should detail the process for identifying whether personal data has been shared with a third party and the process for notifying them. B.15.b. Procedures and responsibilities for compliance with individual rights should be set out in the information sharing agreement to ensure that the routine sharing is as strictly and formally controlled as possible.	
There are regular data quality reviews of systems and manual records created, processed or stored to ensure the information continues to be adequate for the purposes of processing (for which it was collected)	B.16. Regular data quality checks are carried out across LCC to ensure that records contain adequate and relevant information. However, there is no formal quality assurance (QA) process which is adopted across the Council. This creates a risk of non-compliance with Article 5(1)(c) of the UK GDPR.	B.16. Implement a formal QA process for use across the Council, to ensure records that are created, processed or stored contain adequate and relevant information.	High
Staff are made aware of data quality issues both	B.17. It was reported to ICO auditors that LCC runs ad hoc staff awareness campaigns	B.17. Continue with current practices to raise staff awareness of data quality	Low

Records Management

Control	Non-conformity	Recommendation	Priority
through ongoing awareness campaigns or training, and following specific data quality checks or audits	regarding the quality of data, as well as raising data quality issues in team meetings and staff 121s. It is also included in the mandatory IG level 1 training. However, there are no other data quality awareness raising practices or ongoing campaigns. The risk is that if LCC staff are unaware of ongoing issues, then the Council risks those issues being compounded rather than resolved. This may result in a breach of Articles 5 (1)(c, d, e, f), 5(2), and 32 of the UK GDPR.	requirements and good practice, but also introduce additional tools which will do this on a regular basis for example through newsletters and the Council's communication channels. This will help LCC to gain assurance that staff are aware of existing data quality issues and have been told how they can help to improve the quality of data processed by the Council.	
Information or records (both 'active' records and records in archive) are weeded on a periodic basis to reduce the risk of inaccuracy or excessive retention	B.18. During interviews ICO auditors were informed that weeding is taking place across the organisation on an ad hoc basis; it forms part of the decommissioning process for information systems during the current migration to new systems and when boxes stored within archive are being reviewed to assess their content. There does not appear to be a formal overarching documented policy or process within any policies or procedures for the management of information systems or physical records. If weeding does not take place in all areas of the organisation, there is a risk that information may be retained when it is no longer accurate, relevant, or required. This may breach Article 5(1)(a-f) of the UK GDPR.	B.18. Periodically weed all information systems and physical records (active and archived) containing personal data. This should form part of a programme of weeding activities which are formally documented within a policy and/or procedure. This will ensure LCC is reducing the quantity of personal data held, in order to improve accuracy and reduce excessiveness.	High
There is a retention schedule outlining storage periods for all personal data (this includes manual and electronic records) which is reviewed regularly	B.19. LCC are in the process of reviewing the retention schedule as the Council is aware it is overdue a review and that it is also incomplete. For example, LCC do not have a staff email retention period in place, so whilst staff emails are archived after 12 months, they are not deleted. This means the Council may keep	B.19. Ensure that the review of the retention schedule is completed and that records are identified. The retention schedule must then be adhered to, disposal decisions made and put into effect as soon as possible to avoid retaining information for longer than is necessary.	Urgent

Records Management			
Control	**Non-conformity**	**Recommendation**	**Priority**
and has a designated owner	personal data for longer than needed. Furthermore, when a member of staff changes role in the Council, they may have access to personal data which they should no longer have access to, which could result in a personal data breach. Implementing an email deletion schedule would reduce the opportunity and therefore the risk of this occurring. The retention schedule is not being applied in practice and disposal decisions have not been put into effect. LCC risks retaining information for far longer than is necessary and breaching Articles 5(1)(a, c, e, f), 5(2), and 32 of the UKGDPR.		
The retention schedule is regularly reviewed to ensure that it meets all necessary requirements	See B.19	See B.19	
Electronic Records are disposed of in line with the Retention Schedule	See B.19	See B.19	
Physical records are disposed of in line with the Retention Schedule	See B.19	See B.19	
Appropriate contracts are in place with third parties used to dispose of personal data	B.20. LCC have a contract in place with S2S Electronics, however the copy provided is not signed by either party. The role of the person on the LCC's covering letter does not appear to hold a suitable senior role to authorise the contract. The contract also has an inaccurate expiry date (the contract commenced Wednesday 12 September 2018 and expired	B.20. Ensure there are suitable contracts in place with any third party used to dispose of personal data. Contracts must be signed by a suitable senior staff member in each organisation and should contain accurate and sufficient detail.	High

Records Management

Control	Non-conformity	Recommendation	Priority
	Thursday 12 September 2018). The contract did not contain sufficient detail around the reporting of personal data breaches nor the requirement for the contractor to allow the Council to audit the contractor, and the required timescales and/or notice periods. If appropriate contractual controls are not in place with third parties being used to dispose of personal data, the organisation risks a personal data breach or the inappropriate usage of the personal data by that third party. This may breach Articles 5 (1) (f) and 32 of the UK GDPR.		
There are procedures in place to provide individuals with the 'right to be forgotten' (under the UKGDPR)	See B.14.a - B.14.c.	See B.14.a - B.14.c.	

Personal Data Breach Management and Reporting

Control	Non-conformity	Recommendation	Priority
The organisation has allocated responsibility for assessing, recording and reporting data breaches in a structured hierarchy.	C.01. The job descriptions for the DPO, SIRO and staff members of the IG team do not reflect the responsibilities they have in regard to assessing, recording, and reporting Personal Data Breaches (PDB). If responsibilities are not clearly outlined the council cannot provide assurance that there is a structured approach to decision making on PDBs and there is a risk that the council will make ad-hoc and	See A.01 and A.02 C.01. LCC should update job descriptions to include responsibilities for PDBs, which must be reviewed periodically to ensure that all responsibilities are clearly outlined.	Low

Personal Data Breach Management and Reporting

Control	Non-conformity	Recommendation	Priority
	uninformed decisions which will lead to a potential breach of UKGDPR Articles 33 and 34.		
The organisation has policies and procedures in place to structure its approach to personal data breaches and to provide guidance to staff in the event of an incident.	See A.05 C.02. There is no basic guidance included in the current Incidents Management Protocol for staff who have responsibility for reporting a breach to follow. If staff are unaware of the process, there is a risk that PDBs will go unreported and the Council will not be able to demonstrate compliance with the accountability principle of UK GDPR Article 5.2, or demonstrate compliance under Article 24.	See A.05 C.02. LCC should create basic guidance for staff with responsibility for reporting breaches, to be included in or sit alongside the Incidents Management Protocol. The guidance should include how to report a PDB and a link to the Information Security Incident Reporting form. This will ensure there is a structured approach to reporting personal data breaches in event of an incident.	Medium
Staff with responsibility for processing personal data are able to recognise and escalate personal data breaches.	See A.08 and C.02 C.03. LCC is not employing adequate measures to assure itself that staff who do not have access to a computer are receiving adequate IG training. Without adequate training staff may be unable to recognise a PDB and there is a risk that not all breaches will be reported.	See A.08 and C.02 (a) C.03. LCC must ensure they obtain assurance that staff who do not have access to a computer have completed adequate IG training, appropriate to their level, which covers recognising and escalating PDBs.	Low
Decision makers are equipped to make informed decisions over personal data breaches.	See A.09 C.04. There has not been recent specialised training provided to staff within the IG team to enable them to make informed decisions when assessing PDBs. If decision makers are not adequately trained to assess breaches, LCC risks non-compliance with UK GDPR Article 5(1)(f), 33 and 34 and the possibility of breaches not being reported to the ICO.	See A.09 C.04. LCC should ensure that all decision makers within the IG team are provided with specialised training. This would ensure that all decision makers receive suitable training to help them make informed decisions when assessing PDBs. The ICO has created guidance on training and awareness for specialised roles which can be found on their website.	Medium

Page 114

Personal Data Breach Management and Reporting			
Control	**Non-conformity**	**Recommendation**	**Priority**
Arrangements are in place with joint data controllers in the event of a personal data breach.	C.05. During the ICO audit interviews LCC was not able to provide assurance that breach communication channels and procedures between joint data controllers have been tested. If communications channels are not being tested the council may infringe UK GDPR Article 26.	C.05. LCC should ensure that breach communication channels and procedures between joint controllers have been tested to ensure that the council has taken steps to establish a coordinated approach with any joint data controllers with whom it shares personal data and who may be involved in the breach.	Low
Contracts in place between the data controller and any processors working on their behalf reflect the processor's obligations in the event of a personal data breach.	C.06. Within the standardised contract template there is no nominated point of contact in the event of a PDB, instead it states the third party should "contact the council", which could result in breaches not being directed to and addressed by the IG team. If the contract does not contain specific details outlining the processors obligations and procedures to be followed, there is a risk that the organisation will infringe Article 28 of the UK GDPR and PDBs not being reported.	C.06. LCC should include within the standardised contracts a nominated person of contact. This would ensure that the data controller knows who to contact in the event of a PDB. Please see guidance on what needs to be included in a contract on the ICO website.	Low
Measures are in place to assess the severity of personal data breaches.	C.07.a. LCC did not provide a record of all the categories of personal data it holds, and without this LCC cannot proactively assess the risk to individuals where data in those categories is breached. Without a proactive understanding of the inherent risk in the data being processed, or a rationale behind any assessments made, in the event of a PDB LCC may fail in this obligation and be in breach of Article 33 and separate infringements of Article 5(f), Article 32(2), and Article 33. C.07.b. LCC provided evidence of information risks that have been added to their Corporate	C.07.a. LCC should create a complete record of categories of personal data it holds and have a documented set of criteria in place to assess the severity of the breach and the likely effect on individual’s rights and freedoms. This should reference guidance, for example ICO PDB criteria (likelihood and severity) or ENISA methodology and should provide particular guidance over how to assess a 'high risk' to affected individuals C.07.b. LCC should ensure that staff members with responsibility for proactively	Medium

Personal Data Breach Management and Reporting			
Control	**Non-conformity**	**Recommendation**	**Priority**
	Risk Register and a screenshot of their Information Management Risk Register. However, it was highlighted during interviews that not all staff members working closely with PDBs were aware of LCC's Risk Registers and whether or not highlighted risks from PDBs are added to them. If staff do not have a thorough understanding of LCC's Risk Registers, they will not be able to assess the severity and impact on the affected individuals and there is a risk that a PDB will not be reported to the ICO.	assessing the risk to individuals if a breach should occur are aware of LCC's Risk Registers, including the Information Management Risk Register. Highlighted risks arising from PDBs should be promptly added to the relevant risk register and/or any DPIA that has been carried out, ensuring any new risks are communicated to relevant operational staff.	
An effective and documented logging strategy is in place.	See B.19 C.08.a. LCC does not include retention schedules for data breach logs in their overarching retention documents. They do not define how long they will keep logs of data breaches and whether personal data has been minimised or anonymised during the retention period. Without this policy LCC staff members are not aware how often they have to regularly review breach logs for extensive retention of personal data and the steps they have to take to periodically reduce the personal information held in breach logs through the use of data minimisation or anonymisation techniques. The UK GDPR Article 5 (1)(c) requires that personal data be limited to the purposes necessary in relation to the purposes for which they are processed. C.08.b. During the ICO Audit interviews it was highlighted that the data breach logs are not regularly deleted in line with the retention	See B.19 C.08.a. LCC should update the overarching retention documents to include retention periods, procedures and data minimisation techniques for the data breach logs. C.08.b. LCC must review their data breach logs and delete any personal data that is no longer required, as set out in the retention policy. They need to continue reviewing the PDB logs as laid out in their retention schedule, and could employ dip sampling checks on the data breach logs to test the retention policy is being applied.	High

Personal Data Breach Management and Reporting			
Control	**Non-conformity**	**Recommendation**	**Priority**
	schedule. The UK GDPR Article 5(1)(e) requires that personal data should be no longer than necessary for purposes for which they are processed.		
Procedures are in place to report personal data breaches to the ICO where appropriate.	C.09.a. LCC does not have a 'fall back' procedure for 'out of office hours' breaches. If LCC fail to report a data breach within 72 hours of becoming aware the council is at risk of becoming non-compliant with Article 33 and also may result in a sanction under UKGDPR Article 83 2 (h). In addition to any penalty for the infringements of Article 5 (1) (f) and Article 2. C.09.b. The ICO auditors were not able to determine from the evidence or interviews that discussions held verbally or via email regarding reporting PDBs to the ICO have been documented.	C.09.a. LCC should implement an alternate notification route in the case of a data breach that has been reported out of office hours. This will ensure that the council have appropriate procedures and guidance in place to maintain compliance. C.09.b. LCC should ensure all discussions held verbally or via email regarding reporting PDBs to the ICO should be documented e.g. decisions over not reporting a PDB to the ICO, the reason for any delays and any advice received from the supervisory authority.	Medium
Procedures are in place to notify individuals of a personal data breach where appropriate.	C.10. LCC do not have any templates for services to use to notify an individual of a PDB. It was highlighted during interviews that the service will contact the IG team who will advise the service of the required information that needs to be included in the notification. If LCC do not have processes in place to promptly notify affected data subjects, they will be unable to take necessary precautions resulting in a likely high risk to rights and freedoms. Failure to notify promptly when appropriate in compliance with Article 34 may result in a sanction under Article 83(2) of the UK GDPR, in	C.10. LCC should develop templates to notify individuals of a PDB. They should be made accessible for all services and documented alongside the data breach log to evidence that the individual has been notified and what measures have been put in place to address the PDB. PDB guidance and a checklist for responding to a PDB can be found on the ICO website.	Low

Personal Data Breach Management and Reporting			
Control	**Non-conformity**	**Recommendation**	**Priority**
	addition to any penalty for the infringements of Article 5(1)(f) and Article 32.		
Procedures are in place to investigate security incidents.	C.11. LCC do not document findings when they conduct a formal investigation when a significant breach has occurred, to investigate or ascertain the causes of a breach. Without this evaluation, the council will fail to determine the root cause of the data breach which increases the risk of recurrence. If LCC does not take investigative and corrective action in response to a PDB it is at risk of failing in its obligations under UK GDPR Article 5.1 (f) and Article 5 (2).	C.11. Once LCC has conducted an investigation into a serious PDB, the findings should then be recorded on a risk register once this has been established and reported to senior/strategic management. Once this has been implemented, risks from previous breaches should be periodically re-evaluated, for example when guidance is updated or an encryption method becomes obsolete. This will demonstrate the council processes personal data securely in line with its obligations under Article 5.1(f) and is compliant with UK GDPR Article 5 (2).	Low

Observations

The tables below list observations made by auditors during the course of the audit along with suggestions to assist LCC with possible changes.

Governance & Accountability	
Control	**Observation**

Where the lawful basis is Legitimate Interests, the organisation has conducted a legitimate interests assessment (LIA) and kept a record of it.	Although LCC mainly rely upon public task and legal obligation, they could create a LIA template that can be completed prior to the start of processing if legitimate interests is identified as the most appropriate lawful basis. The LIA could include a consideration of the following: - Not using people's data in ways they would find intrusive or which could cause them harm, unless there is a very good reason; - If processing children's data, ensuring extra care is taken to make sure their interests are protected; - Introducing safeguards to reduce the impact where possible; - Whether an opt out can be offered; - Whether a DPIA is required. This will ensure LCC holds an LIA which is suitably detailed for the context of the council, which is clearly an honest review of the balance of interests. Further guidance on legitimate interests can be found at the ICO website.

Records Management

Control	Observation
The security of manual and electronic records transferred within the organisation and externally to any third party is maintained	The International Data Transfers: Guide for IM&G Practitioners policy is inaccurate in relation to the transfer of information to United States of America. New adequacy regulations came into force on 12 October 2023. A full list of adequacy countries and territories can be found on the ICO website.

Appendices

Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller’s ability to comply with the requirements of data protection legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits

ICO Audit Team

ICO Team Manager – Lauren Sherratt
ICO Engagement Lead Auditor – Luwi Mahenga
ICO Lead Auditor – Kate Oxtoby
ICO Lead Auditor – Emily Dowell
ICO Lead Auditor – Deryn Rhodes

Thanks

The ICO would like to thank Aaron Linden and the IG team for their help in the audit engagement.

Distribution List

This report is for the attention of Aaron Linden (Head of Information Management and Governance & Data Protection Officer) and Mariana Pexton (Director of Strategy and Resources & Senior Information Risk Owner).

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Leeds City Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Leeds City Council. The scope areas and controls covered by the audit have been tailored to Leeds City Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.

Agenda Item 10

Leeds CITY COUNCIL

Report author: Jonathan Foster / Angela Laycock

Tel: 0113 37 88684

Internal Audit Update Report September to December 2023

Date: 12th February 2024

Report of: Chief Officer (Financial Services)

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

Brief summary

This report provides a source of assurance that the internal control environment is operating as intended through a summary of the Internal Audit activity for the period from September to December 2023. The report highlights the incidence of any significant control failings or weaknesses.

The work of Internal Audit contributes to Leeds City Council achieving its key priorities by helping to promote a secure and robust internal control environment, which enables a focus on accomplishing the key priorities and Best City Ambition.

Recommendations

The Corporate Governance and Audit Committee is asked to:

a) receive the Internal Audit Update Report covering the period from September to December 2023 and note the work undertaken by Internal Audit during the period covered by the report;

b) note that there have been no limitations in scope and nothing has arisen to compromise the independence of Internal Audit during the reporting period.

c) Receive the report providing information relating to the Monitoring of Urgent Decisions covering the period September to December 2023.

What is this report about?

1 The Corporate Governance and Audit Committee has responsibility for reviewing the adequacy of the Council's corporate governance arrangements, including matters such as internal control and risk management. The Committee also considers the Council's arrangements relating to internal audit requirements, including monitoring the performance of Internal Audit.

2 This report provides the Committee with a summary of the Internal Audit activity for the period September to December 2023. The work of Internal Audit offers a key source of assurance providing the Committee with some evidence that the internal control environment is operating as intended.

3 The report also includes information relating to the monitoring of urgent decisions which is included to enable timely consideration of these matters by Committee.

Chief Audit Executive Opinion

4 The Chief Audit Executive (this title refers to the Senior Head of Audit, Corporate Governance and Insurance) must deliver an annual internal audit opinion and report that can be used by the organisation to inform its Annual Governance Statement. The annual internal audit opinion must conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control.

5 Consideration of our overall opinion takes the following into account:

- results from the substantive audit assignments we have completed during the period;
- outcomes from our audit work not producing an assurance opinion;
- an assessment as to the timely implementation of internal audit report management actions.

What impact will this proposal have?

6 This report provides a source of assurance that the internal control environment is operating as intended. The report highlights the incidence of any significant control failings or weaknesses that would require the intervention of the Committee.

7 The work of Internal Audit contributes towards Leeds City Council achieving its key priorities and Best City Ambition.

How does this proposal impact the three pillars of the Best City Ambition?

☒ Health and Wellbeing ☒ Inclusive Growth ☒ Zero Carbon

8 The Internal Audit Plan provides assurances that span a range of themes including coverage across the council's three Key Pillars.

What consultation and engagement has taken place?

Wards affected:

Have ward members been consulted? ☐ Yes ☒ No

9 The Internal Audit Plan is developed in consultation with Members and senior management across the authority. Consultation around key risks and priorities continues throughout the year, and continual engagement with directorates is driven through the ongoing completion of audit assignments and the agreement of the associated recommendations.

10 We are currently refreshing our risk assessments ahead of 2024/25 and engaging with key stakeholders across the organisation as we determine our next set of internal audit priorities. Members are asked to consider any areas for inclusion in our ongoing risk assessment. There is a standing agenda item on the Committee Work Programme that provides an opportunity to raise any thoughts around future coverage, and our audit planning report is due to be presented at the March meeting.

What are the resource implications?

11 The Internal Audit Plan includes a number of reviews that evaluate the effective use of resources and provide assurance on the corresponding financial governance, risk management and internal control arrangements.

12 The Internal Audit Update Report also provides the Committee with assurances around the effective use of Internal Audit resources through information pertaining to the delivery and completion of the annual plan.

What are the key risks and how are they being managed?

13 The Internal Audit Plan is subject to review throughout the financial year to ensure that audit resources are prioritised and directed towards the areas of highest risk. This process involves the review of information from a number of sources including the corporate and directorate risk registers.

14 The risks relating to the achievement of the Internal Audit Plan are managed through ongoing monitoring of performance and resource levels. This information is reported to the Committee.

What are the legal implications?

15 The Chief Officer (Financial Services), as the council’s Section 151 Officer, is responsible under the Local Government Act 1972, for ensuring that there are arrangements in place for the proper administration of the authority’s financial affairs. The work of Internal Audit is an important source of information for the Chief Officer (Financial Services) in exercising her responsibility for financial administration.

16 The Public Sector Internal Audit Standards (PSIAS) require the Chief Audit Executive to deliver an annual audit opinion and report that can be used by the council to inform its Annual Governance Statement.

17 The Internal Audit Plan includes a number of reviews that provide assurances around the application of the statutory and constitutional framework.

Options, timescales and measuring success

What other options were considered?

18 The work of Internal Audit provides a key source of assurance to the Committee. Additional assurances are obtained through a range of further reports presented to the Committee throughout the year.

How will success be measured?

19 Success can be measured through the delivery of the Internal Audit Annual Report and Opinion. Each quarterly update report will provide an overview of the work completed during the period which contributes towards the Annual Opinion.

20 Further performance measures and drivers are under continual review to ensure that relevant performance information is reported to the Committee throughout the year.

What is the timetable and who will be responsible for implementation?

21 The Internal Audit Plan is in place and is approved annually by the Committee. The Chief Audit Executive is responsible for delivery of the plan.

Appendices

- A – Internal Audit Update Report – Assurance and Consulting Activities September – December 2023
- B – Internal Audit Update Report – Quality and Performance September – December 2023
- C – Monitoring of Urgent Decisions September – December 2023

Background papers

- None

Appendix A

Leeds City Council

Internal Audit Update Report – Assurance and Consulting Activities

Corporate Governance and Audit Committee

12th February 2024

INTERNAL AUDIT UPDATE REPORT 2023/24

1st September 2023 to 31st December 2023

1 Purpose of this report

1.1 This report provides the Committee with a summary of the work completed by Internal Audit during the period from 1st September 2023 to 31st December 2023.The work of Internal Audit offers a key source of assurance providing the Committee with some evidence that the internal control environment is operating as intended.

2 Internal Audit Plan Progress

2.1 The work of Internal Audit is directed by the annual Internal Audit Annual Plan. This has been developed in line with the Public Sector Internal Audit Standards (PSIAS) and has been reviewed and approved by the Committee.

2.2 Throughout the audit year we will develop our Annual Assurance Opinion based upon:

- Work carried over from the previous year.
- Work contained within the 2023/24 Internal Audit Plan that was approved by the Committee in March 2023.
- Unplanned work undertaken in response to emerging risks and priorities.

3 Changes to the 2023/24 Internal Audit Plan

3.1 At the beginning of the year provision is made in the allocation of audit resources for unplanned work, through a contingency. As requests for audit work are received, or more time is required for jobs or changes in priorities are identified, time is allocated from this contingency.

3.2 There have been changes in leadership and the structure of the internal audit team, as well as the economic environment and risk profile of the council changing dynamically in the period since the plan was initially approved. We are constantly reviewing the audit plan to ensure that it aligns to the key risks and priorities for the council and any new and emerging risks. Work is prioritised to ensure that we are able to deliver that which adds the most value to the Council and the S151 Officer.

3.3 Below is a summary of material considerations and changes that have been made to the 2023/24 Internal Audit plan to date. Schools are excluded from this information due to the dynamic nature of this area of the plan.

Assurance Block	Highlights and Changes
Directorate Risks – Children & Families	In this period, we have started to attend Children & Families Financial Health Task & Finish Group meetings. This enables us to provide support and challenge in relation to the directorate's efforts to address the current financial challenge, including the arrangements in place to deliver their savings programme. In the last update report, we notified the committee that we had removed the Transport review as our proposed work has been superseded by work being undertaken within the directorate. Following attendance at Children & Families Delivery Board and conversations with key members of staff it was agreed that to support the service in their work Internal Audit would undertake an end-to-end review of the transport process, including the flow of data between services. This work has commenced during this period. The audit plan includes time for a review of Care Decisions. We have held discussions with the directorate leadership team and have agreed that this work is no longer an immediate priority as additional controls have been implemented in relation to care decisions as a result of the financial challenge.
Directorate Risks – ICT & Information Governance	In this period, we have commenced a review of the Essential Services Programme (ESP) which is a continuous annual programme of upgrade and refresh of Leeds City Council's extensive core ICT infrastructure. The objectives of the review are to provide assurance that there are adequate arrangements in place to evaluate and select projects for inclusion in the programme, that the programme is appropriately monitored in terms of performance, benefits and outcomes. We have also commenced a review of the Purchase of Non-Standard IT Equipment. The objective of this review is to ensure that there is appropriate governance around the decision to purchase the equipment and that there is appropriate management and security of the actual equipment. This has opened up discussions on how we can support the evolution of digital governance more broadly. We included time in the plan to support the service with their preparation for the ICO visit and will provide support and challenge to the service in their response to the outcomes from this. The audit plan includes time for a review of the Major Incidents process. Our recent reviews of Business Continuity Management and Cyber Security Risk Management have provided assurance in relation to this process, therefore additional work is not required at this stage.

Assurance Block	Highlights and Changes
Other Directorate Risks – City Development	In this period, we have commenced a follow up review of High Value Stock. The review will provide assurance that previous recommendations have been implemented and is being used as a pilot for our recommendation tracking sample checking process.
Other Directorate Risks – Finance & Key Financial Systems	In this period we have issued a report on Budget Monitoring and Control review which contributes to assurances around the arrangements in place to embed the Budget Management Accountability Framework. Recommendations have been agreed that are linked to the implementation of Microsoft Dynamics. The progress in implementation of these recommendations will be monitored through attendance at various Core Business Transformation forums and through our recommendation tracking process. The work we have been undertaking in respect of the ongoing Financial Challenge encompasses various observations and actions that will combine to support and challenge directorates in the achievement of Budget Action Plans, therefore further work is not anticipated under this heading in the current year.
Other Directorate Risks – Procurement	Several pieces of contract management review work are currently ongoing. These reviews have provided the opportunity to cover assurances in respect of both contract specifications and due diligence processes.

4 Final Internal Audit reports issued.

4.1 We have issued 24 audit reports during the period from 1st September 2023 to 31st December 2023.

4.2 Depending on the type of audit review undertaken, an assurance opinion may be assigned for the control environment, compliance, and organisational impact. The control environment opinion is the result of an assessment of the controls in place to mitigate the risk of the objectives of the system under review not being achieved. A compliance opinion provides assurance on the extent to which the controls are being complied with. Assurance opinion levels for the control environment and compliance are categorised as follows: substantial (highest level); good; acceptable; limited and no assurance.

4.3 Organisational impact is reported as either: major, moderate, or minor depending on the severity of the issues identified within the audit. Any reports issued with a major organisational impact will be reported to the Corporate Leadership Team along with the relevant directorate’s agreed action plan.

4.4 The following table provides a summary of the reports issued during the period from 1st September 2023 to 31st December 2023 along with the assurances provided where applicable.

Report Title	Audit Opinion			Assurance Themes
	Control Environment Assurance	**Compliance Assurance**	**Organisational Impact**	
Finance and Key Financial Systems				
Business Rates	Substantial	Substantial	Minor	Performance Management, Risk & Resilience, Financial Management, Legislative/Regulatory Compliance, Value for Money
Budget Monitoring and Control	Good	N/a	Minor	Performance Management, Risk & Resilience, Financial Management, Business Innovation & Development, Value for Money, Governance & Decision Making, Legislative / Regulatory Compliance
Children & Families Finance Policies and Use of Section 17 Fund	N/a – memo issued We have undertaken a review of several finance policies within Children and Families to ensure that these are fit for purpose. This has identified a number of opportunities to strengthen the overall control environment. We will be undertaking a review of progress in implementing the recommendations made in 2024/25			Financial Management, Legislative / Regulatory Compliance, Value for Money, Safeguarding
Other Directorate Risks – Adults and Health				
CIS Payments	Substantial	Substantial	Minor	Financial Management, Business Innovation & Development, Risk & Resilience, Legislative/ Regulatory Compliance, Safeguarding

Report Title	Audit Opinion			Assurance Themes
	Control Environment Assurance	Compliance Assurance	Organisational Impact	
Other Directorate Risks – Children and Families				
Safeguarding	Good	N/a	Moderate	Safeguarding, Legislative/Regulatory Compliance, Governance & Decision Making, Partnerships
Other Directorate Risks – Communities, Housing, and Environment				
Housing Application Assessment and Priority Awards	Good	Acceptable	Minor	Legislative/Regulatory Compliance, Governance & Decision Making, Performance Management
Disabled Facilities Grant 2022/23	N/A – Certification of Grant Claim			Performance Management, Financial Management, Anti-Fraud & Corruption
Housing Leeds Assurance – BITMO Information Governance	Good	N/a	Minor	Information Governance, Legislative/ Regulatory Compliance, Partnerships
Other Directorate Risks – Strategy & Resources				
Business Continuity Management	Good	N/a	Minor	Performance Management, Risk & Resilience, Financial Management, Anti-fraud & Corruption, Governance & Decision Making, Legislative/ Regulatory Compliance, Partnerships, Ethics & Culture
Local Authority Bus Subsidy (Revenue) Grant	N/A – Certification of Grant Claim			Performance Management, Financial Management, Anti-Fraud & Corruption
Other Directorate Risks – ICT & Information Governance				
Cyber Security Risk Management	Acceptable	N/a	Moderate	Cyber Security, Risk & Resilience, Information Governance, Legislative/Regulatory Compliance

Report Title	Audit Opinion			Assurance Themes
	Control Environment Assurance	Compliance Assurance	Organisational Impact	
Other Directorate Risks – City Development				
National Productivity Investment Fund (ORR) Cycleway Grant	N/A – Certification of Grant Claim			Performance Management, Financial Management, Anti-Fraud & Corruption
Schools				
School Voluntary Fund x 8	N/A – Certification of account balances			Financial Management, Anti-Fraud & Corruption, Procurement, Contracts & Commissioning, Value for Money, Governance & Decision Making
Primary School 1 Follow Up	Acceptable	Limited	N/A	Financial Management, Anti-Fraud & Corruption, Procurement, Contracts & Commissioning, Value for Money, Governance & Decision Making
Primary School 1	Acceptable	Limited	N/a	Financial Management, Anti-Fraud & Corruption, Procurement, Contracts & Commissioning, Value for Money, Governance & Decision Making
Primary School 2	Acceptable	Limited	N/a	Financial Management, Anti-Fraud & Corruption, Procurement, Contracts & Commissioning, Value for Money, Governance & Decision Making
Primary School 3	Good	Acceptable	N/a	Financial Management, Anti-Fraud & Corruption, Procurement, Contracts & Commissioning, Value for Money, Governance & Decision Making

4.5 During this period, we have also undertaken a number of reviews for external clients which are not included within this report.

5 Summary of Audit Activity and Key Issues

5.1 During the reporting period, there have been no limitations to the scope, and nothing has arisen to compromise our independence.

Limited or No Assurance Opinions and Follow Ups

5.2 Of the audit reviews finalised during the period, no weaknesses have been identified that would result in “major” organisational impact and no reviews have been issued with no assurance opinions.

5.3 Our protocols specify that we undertake a follow up review where we have previously reported “limited” or “no” assurance for the audited area.

Primary School Audis and Follow Ups

5.4 We previously undertook a review of a primary school that resulted in a limited assurance opinion for both the control environment and compliance opinion. The audit highlighted gaps in the Governing Body’s ability to provide effective challenge during budget setting and budget monitoring. Whilst our follow up identified some improvements in the control environment, in particular relating to financial governance arrangements, issues have continued with regard to compliance. Similar issues have also been identified across other school audits during the period. In all cases, recommendations have been agreed with the Head Teachers and will be followed up.

5.5 Our established risk assessment process has steered us towards auditing specific schools in which it was clear that opportunities may exist to improve on practices, and our observations and recommendations enable value to be added at those particular establishments. The presence of the issues highlighted should not, however, be taken to reflect more systemic weaknesses across other schools. We maintain a watching brief across schools and are currently reflecting on our risk assessment process and the ways in which we can maximise the assurances derived from our coverage.

6 Recommendation Tracking

6.1 There is a process in place aimed at tracking the implementation of high and medium priority recommendations raised within our audit reports. This work is key to helping us understand where controls have been strengthened following our audits and also highlighting areas where we may want to re-visit the activity to ensure actions are being progressed appropriately. Currently all audits that receive a no or limited assurance opinion either overall or for a particular objective are subject to a further audit review, which includes reviewing the progress in implementing the recommendations raised within the previous report.

6.2 The table below details the number of recommendations that have been closed and created during the reporting period and those still ongoing for the period from 1st September 2023 to 31st December 2023. The opening position is based on the figures reported to the committee in September 2023 in the Internal Audit Update Report and is all recommendations that were either not due or outstanding.

Priority	All Outstanding Recs at September 2023	Recs closed to December 2023	Recs opened September to December 2023	Total at December 2023
High	66	52	41	55
Medium	25	34	22	13
Total	91	86	63	68

6.3 Members have requested indicative information on how long recommendations had been overdue. The table below shows a breakdown of open recommendations by Directorate and age.

Assurance Block	Open Actions not due			Actions where target date has been missed by:												Total Open Recommendations At 31st December 2023		
				Less than 3 months			3 to 6 months			6 – 12 months			More than 12 months					
	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total
Children & Families	8	4	12	1	0	1	3	0	3	0	0	0	0	0	0	12	4	16
Procurement	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Adults & Health	0	0	0	2	0	2	3	0	3	4	0	4	0	0	0	9	0	9
Communities, Housing & Environment	8	1	9	0	0	0	0	0	0	0	0	0	0	0	0	8	1	9
City Development	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
ICT and Information Governance	6	1	7	0	0	0	0	0	0	0	0	0	0	0	0	6	1	7

Assurance Block	Open Actions not due			Actions where target date has been missed by:												Total Open Recommendations At 31st December 2023		
				Less than 3 months			3 to 6 months			6 – 12 months			More than 12 months					
	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total	High	Medium	Total
Finance & Key Financial Systems	5	3	8	0	0	0	1	0	1	0	0	0	0	0	0	6	3	9
Resources	11	2	13	0	1	1	0	0	0	0	0	0	0	0	0	11	3	14
Schools	0	0	0	1	0	1	1	0	1	1	0	1	0	0	0	3	0	3
Total	**38**	**12**	**50**	**4**	**1**	**5**	**8**	**0**	**8**	**5**	**0**	**5**	**0**	**0**	**0**	**55**	**13**	**68**

6.4 We have reviewed the recommendations where the target date has been missed to determine if there are any themes that may have led to the delays in implementation.

6.5 Part of the process of updating the recommendation trackers includes determining whether the target dates that were set when the reports where issued are still achievable or whether they may require revision. This is particularly relevant where it is clear that progress is being made, but there are evident reasons why an action cannot practically be completed yet. During this period we have reviewed target dates for a number of recommendations where completion is dependent upon the finalisation of a digital solution in progress. It is often the case that the resourcing requirements and complexity for digital solutions becomes evident once work has commenced, in which case we consider a revision to the target date as appropriate so as to retain an ongoing focus on progressing the implementation of the recommendation. All revisions to target dates have been discussed with the service and agreed with the Chief Audit Executive.

6.6 For all recommendations where the target date has been missed by more than three months, management within the service area have confirmed that the implementation of these is in progress. We appreciate that balancing resources and conflicting priorities is a challenge for all colleagues across the organisation, and the recommendation tracking process helps keep actions in focus where they need to be. Within the Adults & Health assurance block, a number of the actions recorded as still outstanding relate to the Debt Recovery review, and we have just commenced a follow up of this. As part of this work we will review the progress made in implementing the recommendations and where appropriate raise further recommendations to ensure that action is taken to address the issues identified.

6.7 The onus continues to be on directorate and service leads to update the trackers and ensure we have accurate information to analyse and report on. We continue to embed the process effectively and are proactively obtaining feedback to use this in the ongoing development of the tracking process. As directorate engagement improves, we will be introducing a sample checking process moving forward.

7 Other Audit Work

Audit Work Completed	Details	Work Completed This Period	Assurance Themes
Core Business Transformation – Work Packages	Provision of support to various work streams within Financial Services that have been set up to ensure that working practices are fit for purpose and in preparation for the introduction of the new core system.	We have provided consultancy work through the Finance Design Authority to aid in the development of the new processes within Microsoft Dynamics. This has been through a check and challenge role to support the service and ensure that potential risks and control weaknesses are highlighted and considered in the service redesign. We have provided consultancy work through the Core HR / Payroll Design Decision Panel to aid in the development of new processes within iTrent. This has been through a check and challenge role to support the service and ensure that potential risks and control weaknesses are highlighted and considered in the service redesign. We have also provided consultancy work through direct involvement in working groups on the interfaces between dynamics and Civica Pay.	The work contributes across a range of assurances including financial management, risk management, governance & decision making, business innovation and development, procurement, social value, value for money and Legislative / Regulatory Compliance.

Audit Work Completed	Details	Work Completed This Period	Assurance Themes
Core Business Transformation – Programme Assurance	Ongoing work to provide review, advice and challenge to the Programme Board including oversight and advice around the procurement process. The finance solution has been identified and KPMG have been appointed to assist officers in implementing the system. The procurement exercise to procure new Core HR and payroll technology alongside an Implementation and Transformation Partner is complete and Midland HR International have been appointed to implement their iTrent system.	We have presented one quarterly assurance reports to the Programme Board focusing on support and maintenance for the systems post go live and contract management across the programme. We have attended a variety of meetings including the Programme Board to provide review, advice and challenge. The Head of Finance – Internal Audit is the chair of the Delivery and Quality Assurance board set up for the implementation of finance solution. The purpose of this board is to assess project delivery performance and escalate any areas of concern to the Project Steering Group	The work contributes across a range of assurances including financial management and control, risk management, governance and decision making, programme management and contracts and procurement.
Project Management	Ongoing work to provide support and challenge to the service in the development in the new arrangements for the management of ICT projects.	We have provided advice in relation to the contract management for the Resource Augmentation Framework contract and reviewed the draft documents.	The work contributes across a range of assurances including project and programme management, governance and decision making procurement, contracts and commissioning and business innovation and development.

Audit Work Completed	Details	Work Completed This Period	Assurance Themes
Children & Families Delivery Board	Attendance at a board set up to oversee the plan for guiding Children &Families improvement work during the period of transition out of the pandemic and recovering from its impacts	Attendance at several programme board meetings. Specifically we have provided internal audit input into the transport review being carried out by the service. We are supporting the service by undertaking an end to end review of the transport process, including the flow of data between services.	The work contributes across a range of assurances including financial management and risk and resilience, governance and decision making, project and programme management, business innovation and development, and transformation.
Children and Families – Families First Grant Validation	Grant claim validation work carried out to support the Directorate.	We were able to confirm the validity of the claim.	The work contributes to assurances in respect of financial management and governance.
Leeds Building Services Review	A task and finish group has been established to support service improvement within LBS. The group has 5 overarching workstream: IDS, quality management system, procurement, procurement, budget, and workforce. Internal Audit are providing attendance, support, and challenge across a number of these workstreams.	Attendance at several workstream update meeting and overarching group meetings. Specifically, we have also provided input into process mapping exercise under the quality management system workstream.	Financial Management, Business Innovation and Development, procurement, contracts, and commissioning
Purchasing Cards	In depth review of purchasing card transactions, including areas of high spend, choice of suppliers and opportunities to reduce spend.	We have supported the S151 officer with the current financial challenge, highlighting areas where action can be taken regarding purchasing cards to reduce spend.	Financial management, contracts and commissioning, value for money, risk and resilience.

Audit Work Completed	Details	Work Completed This Period	Assurance Themes
		This has resulted in: • A reduction in the number of purchasing cards in use. • Targeted communication to remaining purchasing card holders and approvers to reinforce the spend freeze and spending money wisely value where spend is essential. • Ongoing work with procurement to increase both efficiencies in payment processes for essential goods and services and the value of the rebate received from the card provider.	
Financial Regulations	Contribution to the review of the Council's Financial Regulations	We have contributed to the cyclical review of Financial Regulations to ensure that key audit observations and recommendations are appropriately considered within the control environment. This has also included a review of ownership and oversight of the regulations.	The work helps to ensure that the Council's Financial Regulations remain up to date and fit for purpose.
General audit queries and advice issued	Over the course of the recent period, we have received and responded to a number of queries and requests for advice from departments and service areas. These have covered a range of themes and areas.	The dialogue with service areas demonstrates how respected and valued the Internal Audit service is. It also provides a level of procedural oversight and a source of intelligence to feed into the audit planning process.	The work contributes to assurance in a range of areas, in particular governance and decision making and financial control.

8 Other Audit Activities

Audit Activity	Description
Client Liaison Activities	Provision of professional advice to officers, including client liaison activities that promote the work of Internal Audit, and to reinforce the importance of robust controls and good governance.
Board, committee and working group attendance	Attendance at various boards, committees and working groups including Directorate and Service Leadership Teams. Key boards, committees and working groups are noted in the other audit work table above.
Corporate Governance and Audit Committee support	Drafting reports and attending meetings of the Corporate Governance and Audit Committee. Responding to member queries.
Audit and Risk Updates	Regular meetings between the Head of Audit and the Intelligence and Policy Service to share information around a number of areas that contribute to the risk management process.

9 Counter Fraud and Investigations

9.1 The Corporate Governance and Audit Committee receives a separate report summarising the general activities and work plan of the Internal Audit Counter Fraud Team, including both proactive work and fraud and irregularity investigations undertaken.

This page is intentionally left blank

Appendix B

Leeds City Council

Internal Audit Update Report – Quality and Performance

Corporate Governance and Audit Committee

12th February 2024

INTERNAL AUDIT UPDATE REPORT 2023/24

1ST September 2023 to 31st December 2023

1 Purpose of this report

1.1 This report provides the Committee with a summary on the various activities that provide assurance on the performance and quality of our work along with the continuous improvement of the section.

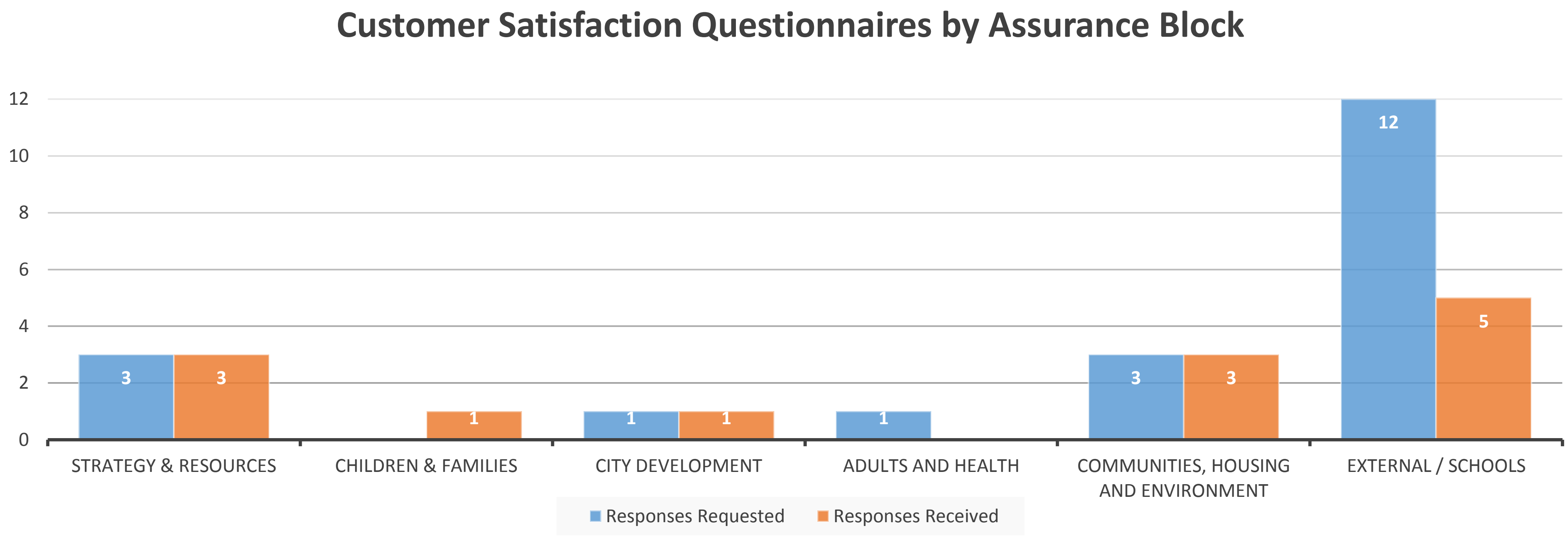
2 Internal Audit Performance

Feedback

2.1 We actively monitor our performance in a number of areas and encourage feedback. A customer satisfaction questionnaire (CSQ) is issued with every audit report. The results of the questionnaires are reported to the Audit Leadership Team and used to determine areas for improvement and inform the continuing personal development training programme for Internal Audit staff.

2.2 In response to member feedback, we have continued to look at ways of maximising CSQ feedback. We now have a fixed deadline by which we would expect feedback to be returned, and we have implemented a chasing process where this is not the case. We have also been looking at the way in which the information is reported.

2.3 We are now reporting on the number of CSQs that have been issued and returned within the specific period. For the period from 1st September 2023 to 31st December 2023 we have issued a total of 20 Customer Satisfaction Questionnaires and received 13 completed returns at a response rate of 65% in the period. The response rate for the previous period was 79%. The majority of the unreturned CSQs relate to schools and specifically School Voluntary Fund audits. These are carried out on request of the school therefore satisfaction with the work undertaken can be implied.



2.4 Below is a summary of comments we have received from services that have completed the CSQs.

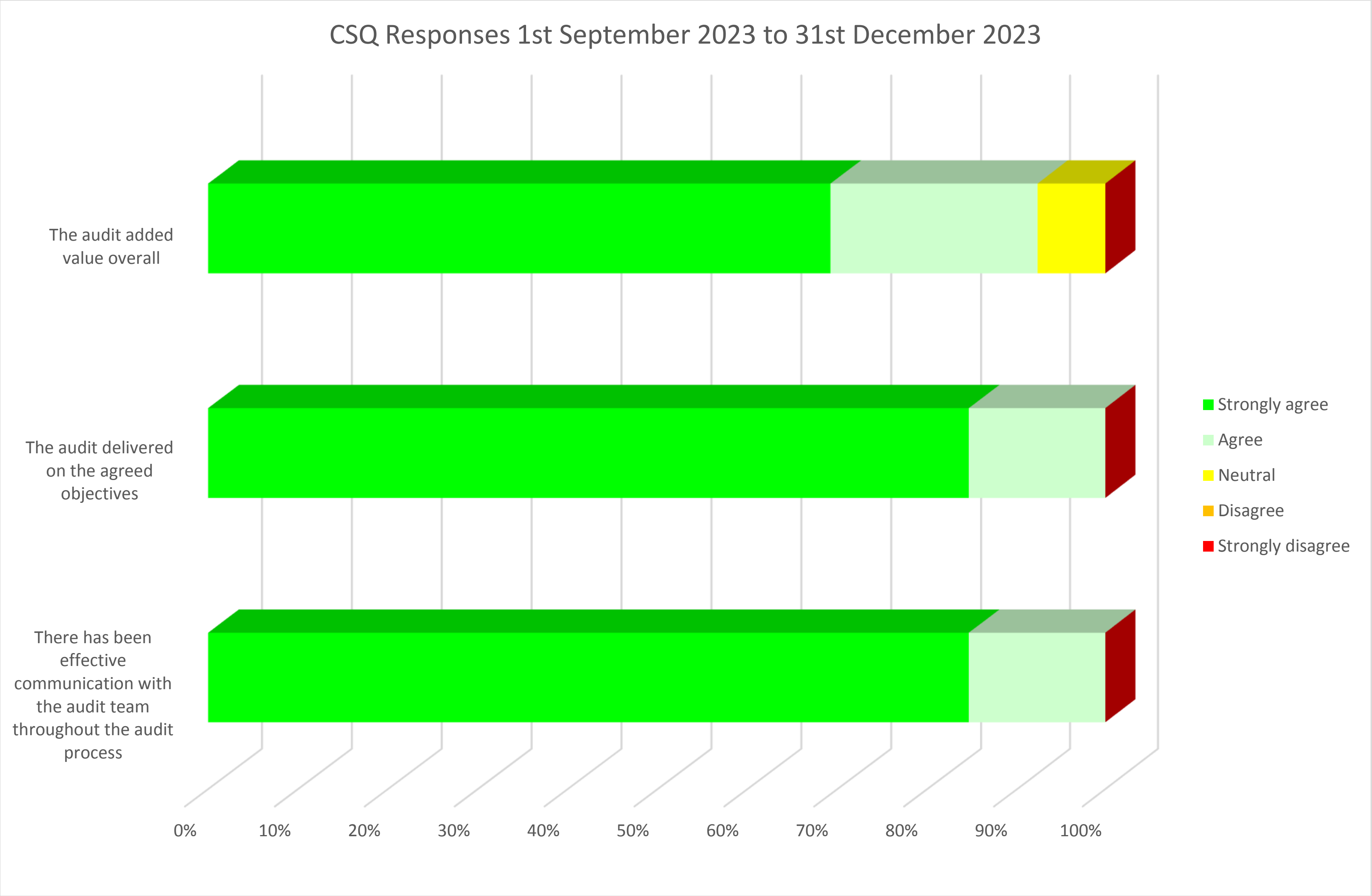
"Regular and supportive communication that maximised both parties understanding of the processes of the service and the auditor. This added value to the audit and helped the service share a maximum amount of context that we work within."

"Open and honest. very professional"

"Very helpful and effective staff"

"This was professionally undertaken with really good levels of consultation and minimal impact on service delivery."

2.5 The graph below shows the responses for each question. In all cases, for all questions, the respondents have selected either strongly agree or agree.



3 Quality Assurance

3.1 Internal Audit work is undertaken in accordance with internal quality procedures incorporated in the quality management system, which has been ISO (International Organisation for Standardisation) certified since 1998. In November 2022 following the external assessment our ISO Quality Management System certification was renewed. This provides assurance that our quality management system continues to meet the requirements of the ISO (9001:2015) standard and is demonstrating continual improvement.

3.2 We have established Quality Assurance procedures within the Internal Audit team. This includes a Quality and Operational Review Group (QORG) that meet to identify and champion improvements in performance and working practices. As part of this process, the Quality Assurance and Improvement Programme (QAIP), which is a requirement of the Public Sector Internal Audit Standards, is in place to bring together our commitment to continually reviewing and improving the way we deliver our internal audit service and embed our quality system.

Action	Timescale and Status
Assurance mapping will continue to be developed to support the annual audit planning process.	Ongoing – We are currently reviewing the audit planning process itself and how we obtain and evaluate assurances and movements in risk throughout the year. We aim to have a refreshed approach in place for 2024/25.
Internal Audit Performance Monitoring – internal performance measures, including KPIs, have been reviewed to support and drive completion of the annual audit plan.	Ongoing – Further work is being undertaken with the aim of reviewing performance measures and producing meaningful information for the committee. We have reflected on the feedback provided by members of the committee. We have developed a to utilise to strengthen performance management and presentation of outcomes. This will be reviewed on an ongoing basis to ensure that it provides the most relevant information for monitoring performance. Changes have been made in the information being reported to committee in relation to recommendation tracking and also customer satisfaction.
Internal Audit Reporting Protocols – to update and streamline directorate reporting protocols to drive timely completion of audit reports.	Ongoing – The protocols have been refreshed and will be relaunched following consultation. We aim to have these established ready for the start of 2024/25. We are continuing to look at the most effective ways of developing and embedding our up-to-date audit protocols.
Automation of the recommendation tracking process – to create an automated process for gathering data on the audit recommendation trackers for each assurance area.	Ongoing – Work has progressed on the creation of an automated audit recommendation tracking process that will lessen the administrative burden that exists currently to collate recommendation tracking data.

Action	Timescale and Status
Engagement – To further increase our presence at key forums to enable closer working across the Council, promote the work of the section and obtain information on any emerging areas of risk or concern.	Ongoing – we have identified a number of forums where our engagement will be helpful, this is an ongoing process. There are a number of actions that we have agreed through the appraisal process that will enable us to take this forward.
New Global Internal Audit Standards – We will undertake a self-assessment against the new standards when they are published and develop an action plan to ensure we will be compliant when the standards become effective.	Not Yet Started – The International Internal Audit Standards Board has approved the new Global Internal Audit Standards which were released on January 9th 2024 and become effective in January 2025. The Public Sector Internal Audit Standards (PSIAS) are based on these. The UK Public Sector Internal Audit Standards Advisory Board (IASAB) will undertake a review of the new global standards. They will seek to determine the implications for the PSIAS as soon as possible and will develop proposals for revised material which will be suitable for the UK public sector context. Any subsequent changes to the UK's PSIAS, and their implementation, will be subject to consultation and appropriate transitional arrangements. Once we understand what these requirements are we will undertake a self-assessment to determine what actions we need to take prior to implementation.

Performance

3.3 We continue to manage our available resources to direct these towards the highest areas of risk to ensure that an evidence-based Head of Internal Audit opinion can be provided on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control in accordance with the PSIAS.

3.4 As we continue to develop and refine our key performance indicators, we will look to incorporate further performance information to demonstrate the effective use of our resources.

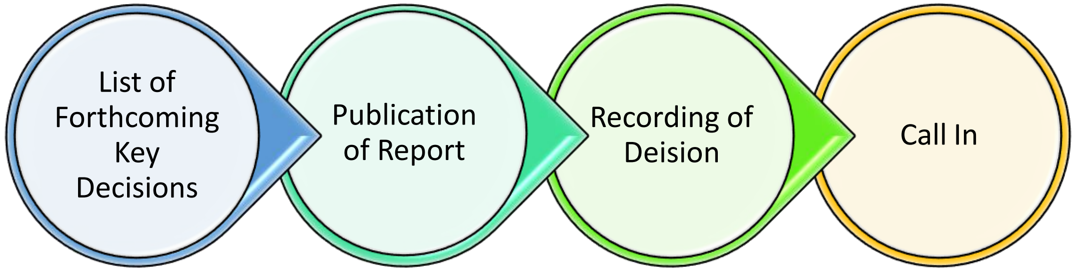
4 Internal Audit Productivity

4.1 The table below shows the progress of the internal audit plan delivery analysed by the number of plan assignments by assurance block. These are assignments where a report is expected to be produced or we are certifying grant balances. It does not include the consultative work, such as attending boards, which is reported in the other assurance work in appendix A.

Assurance Block	**2023/24 plan assignments**	**Plan assignments completed**	**Plan assignments in progress**	**Plan assignments not started**
Grants	18	15	1	2
ICT & Information Governance	7		3	4
Finance & Key Financial Systems	7		3	4
Procurement	2		2	
Adults & Health	4	1	1	2
Children & Families	3		1	2
Other Directorate Risks	16		8	8
Schools	21	16	4	1

4.2 It is evident that a number of pieces of work have not been started. It should be noted that the plan set in March 2023 was based on a resource position significantly in excess of the resource available. This has led us to review how we deliver the work within the plan most effectively. In addition, as is reported in appendix A, a number of pieces of work have been added to the plan to reflect the change in the risk profile of the authority during the year. It is inevitable that not all planned work will be delivered this year and any reviews not started will be rolled into 2024/25 for consideration in the plan through our ongoing risk assessment process. We are currently refreshing our risk assessments ahead of 2024/25 and engaging with key stakeholders across the organisation as we determine our next set of internal audit priorities.

Appendix C – Monitoring of Urgent Decisions (September to December 2023)



The information below updates Corporate Governance and Audit Committee on the ongoing monitoring of the decision-making framework and will support the assurances set out in the annual assurance report of on the decision-making framework.

The List of Forthcoming Key Decisions (LOFKD)

1. This mechanism ensures publicity is provided before key decisions are taken in accordance with the requirements set out in the Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012. ("The Regulations")
2. In line with the Regulations the Executive and Decision-Making Procedure Rules provide that all potential key decisions must be published to the LOFKD (and a link circulated to all Members) not less than 28 days before the decision is taken unless:
   - The decision fits the statutory General Exception (GE) – in which case notice will be published 5 clear days in advance of the decision being taken (and circulated to all Members); or
   - The decision fits the statutory criteria for Special Urgency (SU) – in which case the relevant Scrutiny Chair will be asked to agree that the decision is urgent and cannot be delayed.
3. A performance indicator reflecting the statutory exemptions, requires that 95% of all key decisions should be published to the LOFKD not less than 28 clear calendar days before the decision is taken.

In the period from 1st September to 31st December 2023:

- **100%** of all Officer Key decision were included on the List of Forthcoming Key Decision (LOFKD)
- **93% (14 of 15)** Executive Board Key decisions were included on the List of Forthcoming Key Decisions with 28 days clear calendar days (LOFKD). *Please see the table at the end of the report for details.*

Publication of Report

4. Publication of a decision report enables both elected Members and the public to see and consider the rationale for a key decision before that decision is taken.
5. There is no statutory requirement to publish reports in relation to officer decisions in advance of those decisions being taken. However, the Executive and Decision-Making Procedure Rules provide for a local (non-statutory) requirement that a report in support of a key decision is published five clear working days before that decision is taken by an officer.
6. The rules allow for the late publication of reports in relation to key decisions with the approval of the relevant Executive Member.
7. Corporate Governance and Audit Committee must receive an annual report giving details of any officer key decisions taken at short notice in this way.

In the period from 1st September to 31st December 2023:

- 34 of 34 (100%) of Key decisions taken by officers were supported by reports which were published five clear working days in advance of the decision being taken.
- 14 of 15 (93%) of Key decisions taken by Executive Board were supported by reports which were published five clear working days in advance of the decision being taken.

Recording of Decision

8. Recording of decisions ensures that those decisions are open and transparent, and that the relevant decision maker can be held to account.
9. Regulation 13 of the Regulations, and in relation to non-executive functions Regulation 7 of the Openness of Local Government Bodies Regulations 2014, require a written record to be published in respect of decisions taken by officers. Arrangements set out in the Executive and Decision-Making Procedure Rules, and Access to Information Procedure Rules respectively, require publication of key and significant operational decisions as soon as reasonably practicable after those decisions are taken.

   For the period 1st September to 31st December 2023, 316 decisions were published, please see below for the distribution of these decision.

	Executive Board Decisions	**Officer Decisions**	**Total**
Key Decisions	15	34	**49**
Significant Operational Decisions (SODs)	22	245	**267**
Total	**37**	**279**	**316**

Call In

10. Section 9F of the Local Government Act 2000 requires that executive arrangements by a local authority include the provision for appointment of one or more Overview and Scrutiny Committees with, inter alia, power to review or scrutinise decisions which have been taken by the executive but not yet implemented. These are known as Call In arrangements and are set locally.
11. Part 5 of the Executive and Decision-Making Procedure Rules sets out the call-in arrangements adopted by Leeds City Council. Rule 5.1.2 sets out details of those decisions which are eligible for call in, and rule 5.1.3 provides that eligible decisions may be exempted from call in where the decision is urgent because any delay would seriously prejudice the Council's or the public's interests.
12. Reflecting the importance of Call In to enable the democratic mandate, a performance indicator has been set with a target of 95% of all eligible decisions to be available for Call In.

In the period from 1st September to 31st December 202, 92% (61 of 66) of eligible decisions were available for Call-In.

Officer Decisions:
34 of 34 Key decisions taken in the reporting period were eligible for Call-In; of which 0 (0%) were exempt from Call-In. A total of 34 (100%) of eligible decision taken by offices were available for Call-In.

Executive Board Decisions
32 of 37 decisions taken in the reporting period were eligible for Call-In; of which 5 (16%) were exempt from Call-In. A total of 27 (84%) eligible decisions were available for Call-In. Please see the table at the end of the report for details.

Decisions Not Treated as Key

13. Regulation 18 of the Executive Arrangements Regulations requires that a relevant Scrutiny committee may require the executive to report to Council if a key decision has not been treated as key.

During the reporting period, no decisions have been referred to a Scrutiny Board as wrongly treated.

Decisions Taken Under Urgency Provisions

14. Decisions taken under urgency provisions (general exception or special urgency; short notice reporting; and exemption from call in) are both lawful and constitutional providing they meet the requirements in relation to approvals and notice set out in the relevant Executive and Decision-Making Procedure Rule.
15. During the reporting period, 7 decisions have been taken under urgency provisions (general exception, special urgency, short notice reporting or are exempt from call-in). Each have been treated in accordance with the relevant procedure rule. The reasons for urgency are set out below.

Decisions taken under General Exception (GE) / Special Urgency (SU)			
DDN / Minute	**Decision Maker**	**General Exception/ Special Urgency**	**Title of Decision** Reason for urgency.
October (Minute 58)	Executive Board Director of City Development	**General Exception**	**Accelerated Property Releases and Disposals** In the context of the Council's current financial position, the Council's property portfolio is continually being reviewed to generate operational savings and capital receipts. The opportunity to progress with additional disposals has recently come to light, but due to the need to progress these for completion within the current financial year, it is essential that work proceeds as soon as possible on the marketing and disposal of the assets to ensure that the receipts are achieved by the end of March 2024. Therefore, if the decision was delayed until the November meeting of Executive Board, this could result in the disposals failing to complete in the current year which would impact upon the current budget forecasts.

Decisions subject to late notice reports		
DDN / Minute	**Decision Maker**	**Title of Decision** Reason for short notice report
Minute 53	Executive Board Director of City Development	**The Implications of the Network North Government Announcement for Leeds** the submitted report was in response to the recent Government announcement regarding Network North, and as such the report was not able to be included within the agenda as published on 10th October 2023. However, given the significance of this announcement, it was deemed appropriate for the matter to be brought to the attention of Executive Board at the earliest opportunity.

Decisions exempt from Call-in		
DDN / Minute	**Decision Maker**	**Title of Decision** Reason for exempt from call-in
Minute 44	Executive Board (Director of City Development)	**Provision of a loan for Leeds Culture Trust to cover Culture Sector Tax Relief claims.** Any delay would impact on the Year of Culture programme and seriously prejudice the public's interests, as the Call-In period extends beyond the time when the payment of the first instalment of the loan is needed.
Minute 52	Executive Board (Director of City Development)	**Transpennine Route Upgrade – Transport and Works Act Order Representation.** The decision is urgent and that "any delay would seriously prejudice the Council's or the public's interests". The ground of urgency is that the resolution from Full Council is required before the Public Inquiry for the Transport and Works Act Order begins, which is estimated to be January 2024. If the decision were to be subject to the Call-In procedure and delayed by the operation of the Call-In mechanism, it may mean that the Council is not able to participate in the Public Inquiry or while we've got arrangements in place already continue negotiations with Network Rail and other Stakeholders to endeavour to reach agreement on outstanding matters.
Minute 70	Executive Board (Director of City Development)	**Friendship Oath with the City of Kharkiv** The International Relations Team had successfully secured some funding from the British Embassy in Prague to cover the full costs of a Mayoral visit to Brno on 1st – 7th December 2023 to celebrate our 20th Anniversary of partnership. This will reduce costs and carbon footprint associated with face-to-face meetings and underline the Council's alliance with its European twinned cities. To secure the funding and ensure signing has taken place prior to deadlines, the decision was requested to be exempt from the Call-in process
Minute 77	Executive Board (Director of City Development)	**Leeds City Council Response on the West Yorkshire Combined Authority Bus Reform Consultation** The report is requested to be urgent and that "any delay would seriously prejudice the Council's or the public's interests". The Consultation was launched by WYCA on October 10th, and consultation events continue around West Yorkshire until December 8th, therefore it was not possible to present this item at an earlier Executive Board due to governance processes.
Minute 79	Executive Board (Director of Children and Families)	**Outcome of statutory notice on a proposal to change the age range at Rothwell Primary School, from 3-11 years to 4-11 years and permanently close the nursery.**

		The Executive Board is the decision maker for this proposal and statutory guidance states that a final decision must be made within 2 months of the end of the statutory notice period, therefore by 3rd January 2024, or be referred to the Schools Adjudicator. The representation period ended on 3rd November 2024 and the earliest that a report could be presented to Executive Board was 13th December 2023. Should the decision be “Called-In” at this point the decision may not have made the deadline of 3rd January 2024. The consequence would be that a local decision could no longer be made, and the matter would automatically be referred to the Office of the School Adjudicator to decide.

Report author: Jonathan Foster

Tel: 0113 3788684

Counter Fraud Update Report April – December 2023

Date: 12th February 2024

Report of: Senior Head of Audit, Corporate Governance and Insurance

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

Brief summary

This report provides a source of assurance that the internal control environment is operating as intended through a summary of the counter fraud activity for the period from April to December 2023. It includes the annual update to the Committee on the Council use of Regulation of Investigatory Powers Act 2000 (RIPA).

The report also presents the updated Anti-Bribery Policy and Policy on a Page.

The work of the counter fraud team within Internal Audit and from other services with counter fraud roles contributes to Leeds City Council achieving its key priorities by helping to promote a secure and robust internal control environment, which enables a focus on accomplishing Best Council Plan objectives.

Recommendations

The Corporate Governance and Audit Committee is asked to

a) receive the Counter Fraud Update Report covering the period from April to December 2023 (Appendix A) and note the work undertaken by Internal Audit and other service areas during the period covered by the report.
b) endorse the Anti-Bribery Policy (Appendix B) and Policy on a Page (Appendix C).

What is this report about?

1 This is a bi-annual update report providing assurance as to the control environment in respect of counter fraud and corruption activity, including the annual update on the Council use of RIPA. The report also presents the updated Anti-Bribery Policy and Policy on a Page.

2 The work of Internal Audit, including the counter fraud function within it, contributes to Leeds City Council achieving its key priorities by helping to promote a secure and robust internal control environment, which enables a focus on accomplishing Best Council Plan objectives.

What impact will this proposal have?

3 The assurance set out in this report will inform the annual audit opinion given by the Head of Internal Audit and provide evidence of the ongoing review of the Council's arrangements for internal control supporting the Council's Annual Governance Statement. This also provides assurances to the Corporate Governance and Audit Committee regarding the robustness of the system of internal control.

How does this proposal impact the three pillars of the Best City Ambition?

☒ Health and Wellbeing ☒ Inclusive Growth ☒ Zero Carbon

4 Arrangements in respect of counter fraud and corruption support the ongoing delivery of the council's three pillars.

What consultation and engagement has taken place?

Wards affected:		
Have ward members been consulted?	☐ Yes	☒ No

5 The Internal Audit Plan, including the counter fraud plan, is developed in consultation with Members and senior management across the authority. Consultation around key risks and priorities continues throughout the year, and continual engagement with directorates is driven through the ongoing completion of investigations and the agreement of the associated recommendations.

6 Updating the Anti-Bribery Policy has involved consultation with colleagues in Legal Services and the Trade Unions.

What are the resource implications?

7 The work undertaken to satisfy the counter fraud and corruption requirements of the internal audit plan do so from within existing resources.

8 The update reports to be received by committee each year provides assurance that effective arrangements are in place to combat the risk of fraud and corruption within the council.

What are the key risks and how are they being managed?

9 The Counter Fraud update report contains details of the key fraud risks and assurances around how they are being managed. Internal Audit are working with risk colleagues to raise awareness of fraud risks at directorate management team meetings. Internal Audit work collaboratively with colleagues with counter fraud roles within the council.

What are the legal implications?

10 The Chief Officer (Financial Services), as the council's Section 151 Officer, is responsible under the Local Government Act 1972, for ensuring that there are arrangements in place for the proper administration of the authority's financial affairs. The work of Internal Audit is an important source of information for the Chief Officer (Financial Services) in exercising her responsibility for financial administration.

11 The Public Sector Internal Audit Standards (PSIAS) require the Head of Audit to deliver an annual audit opinion and report that can be used by the council to inform its Annual Governance Statement.

Options, timescales and measuring success

What other options were considered?

12 The work of Internal Audit including the counter fraud function provides a key source of assurance to the Committee. Additional assurances are obtained through a range of further reports presented to the Committee throughout the year.

How will success be measured?

13 A successful counter fraud and corruption environment will protect the Council's resources, underpin the successful delivery of the Council's strategic objectives, and contribute to the value for money conclusion of the Council's external auditor when reviewing the statutory statement of accounts.

What is the timetable and who will be responsible for implementation?

14 Work is ongoing as set out in the appendix attached.

Appendices

A – Counter Fraud Update Report – April - December 2023

B – Anti-Bribery Policy

C – Anti-Bribery Policy on a Page

Background papers

15 None.

This page is intentionally left blank

Appendix A

Leeds City Council

Counter Fraud Update Report – April to December 2023

Corporate Governance and Audit Committee

12th February 2024

COUNTER FRAUD UPDATE REPORT 2023/24

1st April 2023 to 31st December 2023

1 Background

1.1 Local authorities have responsibilities for the effective stewardship of public money and for safeguarding against losses due to fraud and corruption. The Council has a zero tolerance stance on fraud and corruption. The CIPFA (Chartered Institute of Public Finance and Accountancy) 2018 Guidance on Audit Committees sets out the role of the Audit Committee regarding 'countering fraud and corruption'. In summary, the Committee should understand the level of fraud risk to which the authority is exposed, and the implications for the wider control environment. This can be undertaken by having oversight of counter fraud activity. Effective counter fraud arrangements also link to the ethical standards for members and officers that the public expects.

1.2 This report is designed to help meet this duty and is set out to give assurances to Committee members surrounding the counter fraud activities undertaken during the period April to December 2023.

1.3 Within the audit plan, resources are made available to undertake investigations, or reactive work, to look into identified instances of fraud or theft, and to investigate concerns raised by staff or members of the public. To help to ensure controls are in place to prevent fraud from occurring, we also undertake targeted proactive reviews. These are developed from our understanding of the control environment, in addition to our awareness of new and emerging fraud risks.

1.4 The Public Sector Internal Audit Standards (PSIAS) set out that the primary responsibility for the prevention and detection of fraud lies with management. Auditors should have sufficient knowledge to recognise the indicators of fraud. This is addressed by having experienced auditors with a variety of qualifications, continuing professional development and attendance at targeted counter fraud training. We can never be complacent, as fraud risks continually evolve. We therefore regularly enhance and develop our counter fraud capability by reviewing the tools and techniques that we use to detect and prevent fraud from occurring in the first place.

1.5 In this report, in addition to the work undertaken by Internal Audit, information from other service areas who contribute to the Council's counter fraud assurances is included. This gives a more rounded overview of the work that is being undertaken across the Council on counter fraud activities.

1.6 This report includes the annual update to the Committee on the Council use of Regulation of Investigatory Powers Act 2000 (RIPA).

2 Referrals to Internal Audit

2.1 Internal Audit are the corporate owners of the Council’s counter fraud policies. The channels where concerns can be raised by both staff and members of the public, include the provision of a dedicated inbox, telephone line, post, and a ‘do it online’ form for members of staff. We also receive confidential referrals through other routes such as the Freedom to Speak Up Guardian or those shared by external agencies, for example the National Anti-Fraud Network, or other Council services seeking advice or assistance. The table below illustrates the referrals received by directorate and by the type of the concern raised between April and December 2023.

Directorate						
Referral type	**Adults & Health**	**Children & Families**	**City Development**	**Communities, Housing & Environment**	**Strategy & Resources**	**Total**
Economic and voluntary sector support fraud (Covid and other grants)				1	3	4
Payroll and recruitment fraud						
Staff conduct		2	2		1	5
Safeguarding		2				2
Social care fraud	2					2
Corruption/maladministration			3			3
Theft				2		2
Procurement fraud - Mandate and purchasing cards			1	1	1	3
Non-compliance with policies and procedures		1	1			2
Cheque fraud		2				2
Health and Safety						
Misuse of Council funds						
Value for money						
Debt Fraud					1	1
Council Tax Fraud			1			1
Total						**27**

2.2 The table below compares the number of referrals received by financial year and includes 2023/24 up to the end of December 2023. The referrals received during 2020-21 were higher than those in other years, most notably due to concerns being raised regarding covid business grants and other covid related activity. There was an increase in referrals received in the 2022/23 financial year. This could be attributable to a number of factors, including the increased communication and awareness raising of the channels to raise concerns, the uptake of the fraud awareness training, and the establishment of a Freedom to Speak Up Guardian. We review referrals received on an ongoing basis to feed into the risk based planning of Internal Audit.

2019-20	2020-2021	2021-2022	2022-2023	2023-24 Q1-Q3
46	74	45	61	27

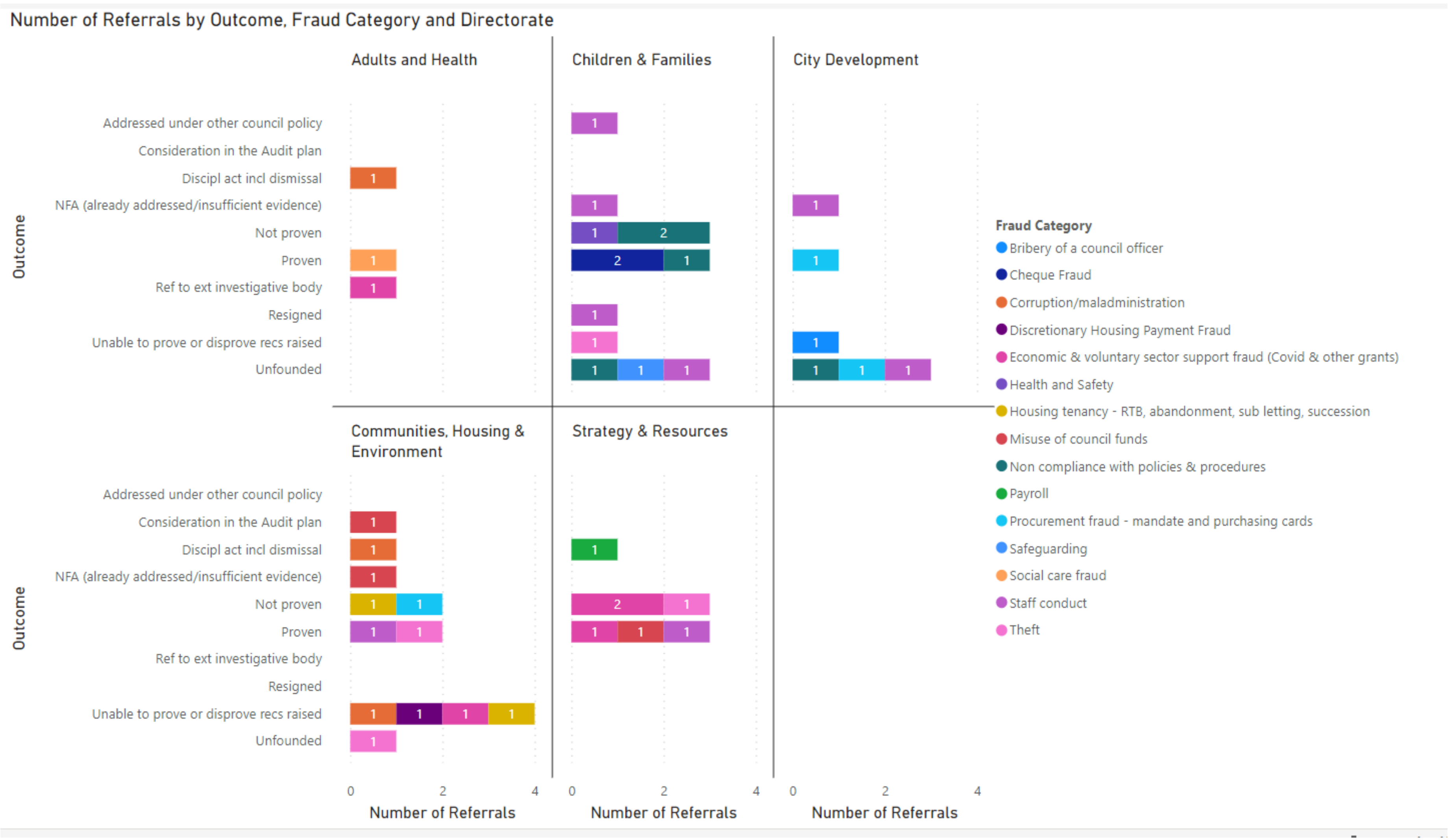
2.3 It should be noted that previously we have reported figures for Housing Tenancy (including RTB and sub-letting) fraud within the above table. These now go directly to the Tenancy Fraud team and are reported separately in this update report at sections 4.2 – 4.5.

Open Investigations

2.4 As at the 31st December 2023, 17 referrals were being investigated. Of these, 10 have been newly opened during the reporting period with the remaining 7 carried forward from previous periods. We regularly monitor open investigations to ensure that these are progressed as swiftly as is practical. However, it is inevitable that some cases will be complex in nature and the length of time that it takes to fully conclude will often be outside our control. Investigations are undertaken by either Internal Audit, Human Resources, staff within directorates or a combination of these. In all cases Internal Audit undertake a risk assessment upon receipt of the referral and determine the most appropriate investigative route. We only close investigations where we are fully satisfied all reasonable lines of enquiry have been exhausted and these are reviewed in line with our quality assurance arrangements.

Closed Investigations

2.5 A total of 41 referrals were closed during the period, this includes some referrals that were received in the previous financial year. The outcomes are shown below by directorate and fraud category. Where appropriate, recommendations are agreed to improve the control environment, and these are tracked and reported though the Internal Audit Update reports to the Committee.


Number of Referrals by Outcome, Fraud Category and Directorate

3 Internal Audit Proactive Counter Fraud Work

3.1 To help ensure that there is an effective counter fraud culture in place within the Council, we undertake various proactive counter fraud activities. Areas of work are highlighted below.

National Fraud Initiative (NFI)

3.2 The NFI is an exercise conducted by the Cabinet Office every two years that matches electronic data within and between public and private sector bodies to prevent and detect fraud and error. Relevant teams within the Council (such as Internal Audit, Welfare & Benefits and Housing and Tenancy Fraud) have been working through the matches on a risk basis.

3.3 Internal Audit has overall responsibility for monitoring the progress of this exercise and ensuring that the NFI system is updated. We are in the process of reviewing the 21,152 matches received for the 2022/23 exercise based on risk. This is an increase from 17,272 quoted in the last report due to release of additional matches.

3.4 To date, twenty issues have been identified resulting in £46,089 currently being in recovery[1]. Review of the output of this exercise is still ongoing.

Counter fraud reviews

3.5 During the period we have carried out specific reviews to address areas of identified fraud risk to the authority. The prioritisation of this work considers the use of best practice and our internal risk assessments. Internal fraud is recognised as a key risk across several publications including Cifas latest Fraudscape report, and Internal Audit activity in these areas acts as a key deterrent in accordance the Council’s zero tolerance approach. The following reviews have been undertaken during this period:

- Mileage Claims

3.6 Several recommendations were made to strengthen the control environment including improvements to communication, and oversight to support the financial challenge. The review also highlighted considerations around the capabilities of new technology through the core business transformation programme.

[1] This relates to Council Tax Reduction Scheme and Housing Benefit claims linked to student loans.

- Purchasing Cards

3.7 This has resulted in several conversations across the Leadership Team along with the production of dashboard information that will strengthen oversight and challenge. Similar work was undertaken around purchasing card transactions in Schools with key observations and findings reported to the individual schools where required.

Awareness Raising

3.8 In addition to the reactive and proactive work, our counter fraud arrangements include regular communications to staff around current fraud risks, and the signposting of where to report any concerns. During the period we have participated in World Whistleblowers Day in June and International Fraud Awareness week in November where we promoted the Fraud Awareness Training [2] on Insite. We also raised awareness of the Fraud and Corruption toolkit, available policies and how employees can report concerns.

3.9 We have also contributed an article to the Contract Manager Newsletter to highlight procurement fraud risk and the importance of effective contract management.

3.10 Regular meetings with the Freedom to Speak Up Guardian (FTSUG) are held where any concerns that are considered to require Internal Audit investigation are discussed, and actions agreed.

3.11 As members of the National Anti-Fraud Network (NAFN) we receive regular intelligence alerts on active or reported frauds experienced by other member bodies. Details of the fraud risks are shared with the relevant service. We also share this knowledge across the wider audit team as part of the audit preparation process so any risks can be considered within the scope of a review where relevant. We continue to work collaboratively with counter fraud colleagues within the Council to share ideas and promote best practice and the fraud awareness training. Developing these relationships will enhance our ability to identify and respond to emerging fraud risks.

Counter fraud policy framework

3.12 As part of our refresh programme of the suite of counter fraud and corruption polices, we have undertaken a review of the Anti-Bribery Policy. The review established that it remains in line with current legislation and as such there have only been minor amendments. This includes:

- Strengthening some specific areas of wording

[2] The Fraud Awareness e-learning training was launched in May 2022, from this time up to the end of December 2023, 785 employees have completed this.

- Aligning the policy with the Council values and expected behaviours
- Including reference to supporting policies and the Fraud Awareness Training
- Including contact details for reporting concerns.

3.13 We have also developed the Policy on a Page which provides the key messages on an easy-to-read document. Both documents will be made available to staff on Insite and will form part of the Fraud and Corruption toolkit.

3.14 The Anti-Bribery Policy and Policy on a Page are appended within this update report for awareness and endorsement.

Moving forward

3.15 There are various other pieces of work ongoing that will provide important assurances around potential areas of fraud risk. Moving forward we are looking at ways to align the counter fraud activities and priorities more closely with the work undertaken across the Internal Audit plan. For example, where emerging fraud risks come to light, we will be looking to utilise the resource across the team to ensure these are considered and incorporated within relevant pieces of Internal Audit work. This will ensure that proactive fraud activity becomes the business of the whole Internal Audit team and maximises synergies across the service.

4 Other areas of assurance

4.1 There are a number of other areas of activity across the Council that feed into the counter fraud assurances. Details of this work is included in the report as follows.

Housing Leeds

4.2 Housing Leeds provides a range of tenant and property related services for Council tenants and leaseholders, private rented sector tenants and homeowners. There are three Tenancy Fraud Officers whose role is to prevent and detect housing fraud to ensure that homes are fairly given to the people who need them. It is a criminal offence to commit tenancy fraud under the Prevention of Social Housing Fraud Act 2013.

Tenancy fraud includes: -

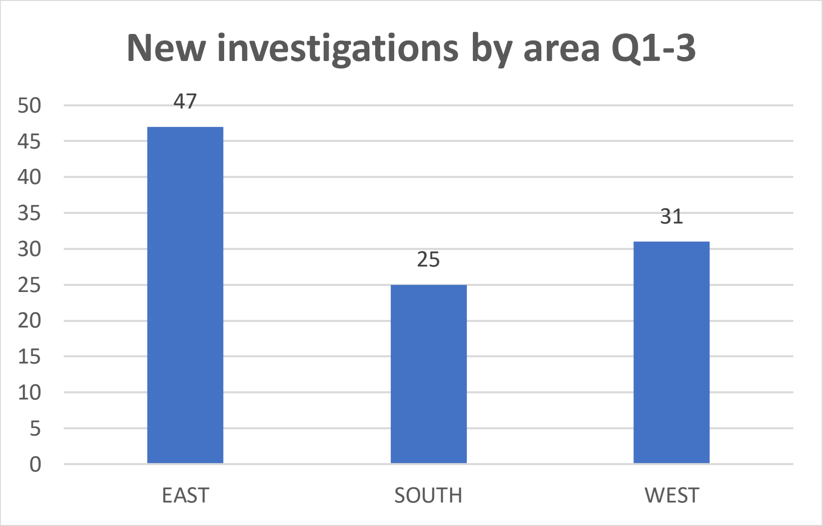
- Application fraud - not telling the truth when applying for a property, for example about how many people live there

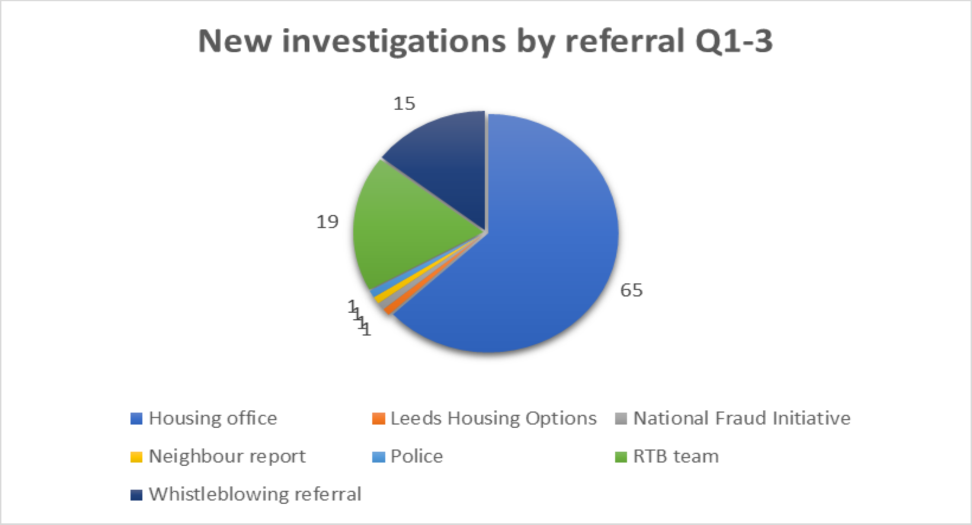
- Subletting fraud - a property is sublet without permission (this is a criminal offence)
- Succession fraud - living in a property after someone has died without the right to do so
- Non occupation fraud - the named tenant permanently living somewhere else
- Right to Buy fraud – false information provided to acquire a property at a discounted price

4.3 The information below summarises the work undertaken between April and September by the Tenancy Fraud Officers.

There were 103 new investigations opened in Qtrs. 1-3. There are currently 104 ongoing cases being investigated citywide.

The majority of referrals received in Qtrs. 1- 3 were made by the housing office (63%) or the RTB team (18%).



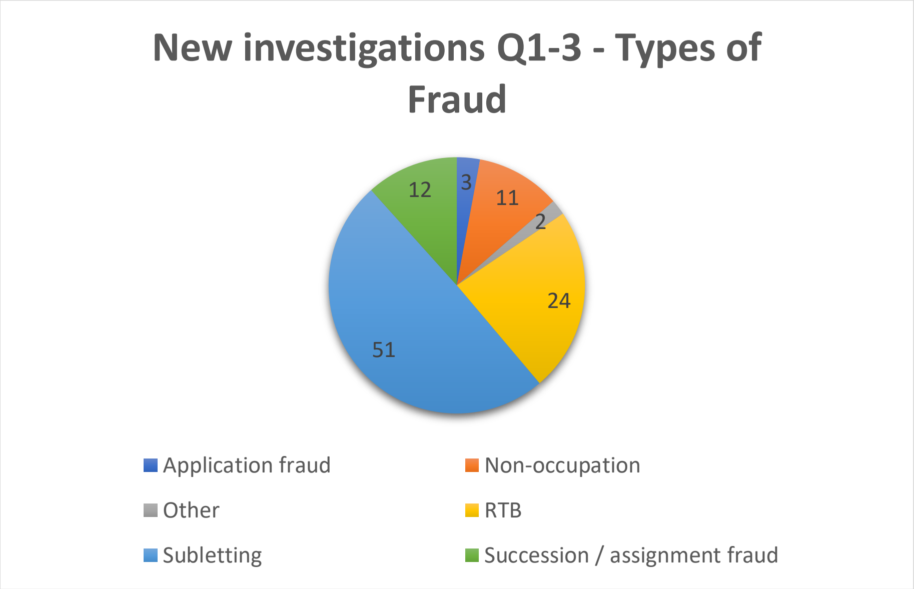


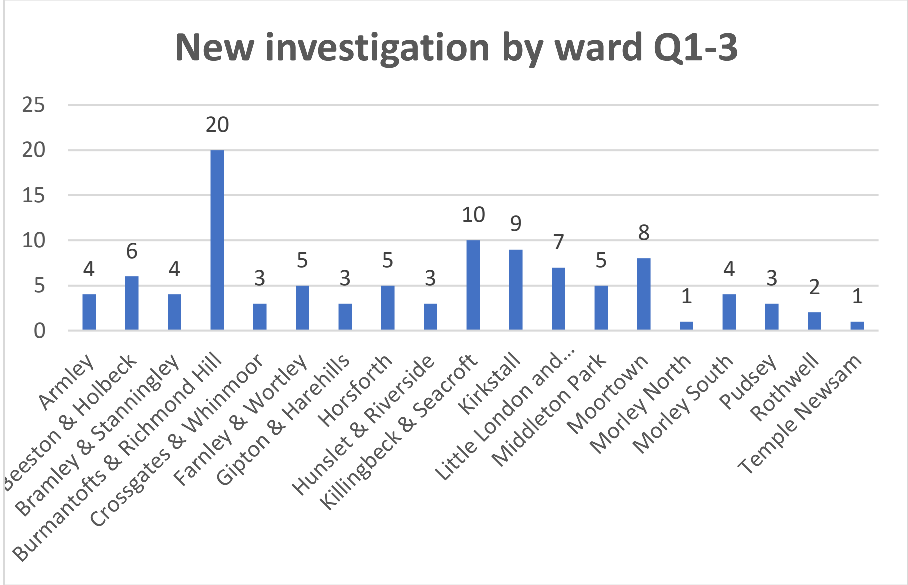
The Tenancy Fraud Officers have continued to prioritise subletting cases and Right to Buy fraud cases.

Subletting has been the most frequent type of investigation in Qtrs. 1-3 (50%) followed by right to buy cases (23%).

The highest number of new cases were opened in the Burmantofts ward.

Investigations were opened in 19 wards across the city in Qtr.1 – 3.





19 council properties were recovered as a result of fraud investigations in Qtrs. 1 - 3. These can be broken down by area as follows:

- East 2
- South 8
- West 9

At the end of Qtr. 3 there were a total of 521 properties recovered since 2008.

The following properties have been recovered in Qtrs. 1 - 3:

- 6 x 1 bed flat
- 1 x 1 bed house
- 4 x 2 bed flat
- 2 x 2 bed house
- 1 x 1 bed multi storey flat
- 1 x 3 bed multi storey flat
- 4 x 3 bed house

4.4 The above information provides the Committee with some assurance that the Council has arrangements in place to identify and address suspected instances of Tenancy Fraud, and that action is taken to recover properties where applicable.

4.5 During the period dialogue has been opened with neighbouring authorities and core cities to share good practices in the management of housing tenancy fraud. We will continue to pursue this work and reflect on notable findings and observations with our colleagues in the housing tenancy team.

Insurance Services

4.6 Insurance Services procures and manages all the Council’s insurance contracts and provides advice and guidance to all Council services. Most claims are paid from the self-funded insurance provision. These claims include public liability claims from members of the public, employer liability claims, property, and motor claims.

4.7 False insurance claims are recognised as a key fraud risk area in the Fighting Fraud and Corruption Locally (FFCL) strategy. A total of 959 claims were received between April and December 2023 and the volume underlines the importance of remaining vigilant to the risk of fraud. The Council has a robust assessment and checking process in place which identifies claims warranting further investigation. The service work with the Legal Services litigation team and external solicitors where cases reach the point for court intervention. The table below illustrates the claims position to date where the claim has been handled by the Insurance and Legal Section, where the cases have reached the threshold for legal intervention, thus providing some assurance over the counter fraud arrangements in this area.

Public Liability Claims				**Employer Liability Claims**	**Motor Claims**
Year claim relates to	Fraud Investigation ongoing	Claims Withdrawn	In Recovery	In Recovery	In Recovery
2017		2	1	1	
2018	4	4		2	1
2019	5	2	1	1	
2020	3	2		1	
2021	3	2			
2022	3				
2023					

4.8 The work that is undertaken by the service, identifies cases where further investigation is required. Where claims have been found to be fundamentally dishonest, this results in funds being paid back to the Council which can then be spent elsewhere. In the cases where the claims are withdrawn, these have ongoing court involvement as we wish to recover any costs incurred on defending the claim, these currently total £32,640. The concept of fundamental dishonesty means that a claim can be dismissed due to concerns surrounding the conduct of claimants (for example submitting false documents to support a claim).

Social Care Fraud

4.9 The Council gives money to both adults and children with care needs to manage their support in a way which best meets their requirements. Direct payment fraud can include falsely claiming or misusing direct payments / personal budgets, either by the service user, carer, relatives, or friends. This is a misuse of Council funds and the direct payment audit team work in partnership with West Yorkshire Joint Services where payments made reach the threshold for criminal investigation. Instances of suspected fraud are to be notified to Internal Audit and these figures are captured in the tables at 2.1 and 2.5 above.

4.10 We previously reported a separate case which was being prepared for prosecution, this has now been resolved, and money is being recovered by the Council.

Welfare and Benefits Service - Council Tax Support and Housing Benefit claims review

4.11 In previous updates we have referenced work to be undertaken as a result of funding provided by the Department for Works and Pensions. This has resulted in a review of 6,300 Housing Benefit claims during 2023/24 to ensure up to date details are held in relation to claimants. These reviews are now complete, and we have been assured that any discrepancies identified have been corrected. The receipt of electronic real time notifications of changes from the Department for Works and Pensions and HMRC mean that there continues to be a lower risk in terms of changes not being identified.

4.12 We have also been advised of the following areas of activity within the service:

- The Welfare & Benefits service were given responsibility for the administration of the Local Welfare Support Scheme during 2023/24 and have subsequently introduced additional measures to help prevent fraudulent applications.
- The service have also undertaken some proactive work during the year to target Housing Benefit claims with additional adults living in the property. As a result of this exercise, £174K in overpaid Housing Benefit has been identified and will be recovered where appropriate.
- Proactive work with colleagues in other council departments is ongoing such as Housing to identify and assess eligibility where appropriate.

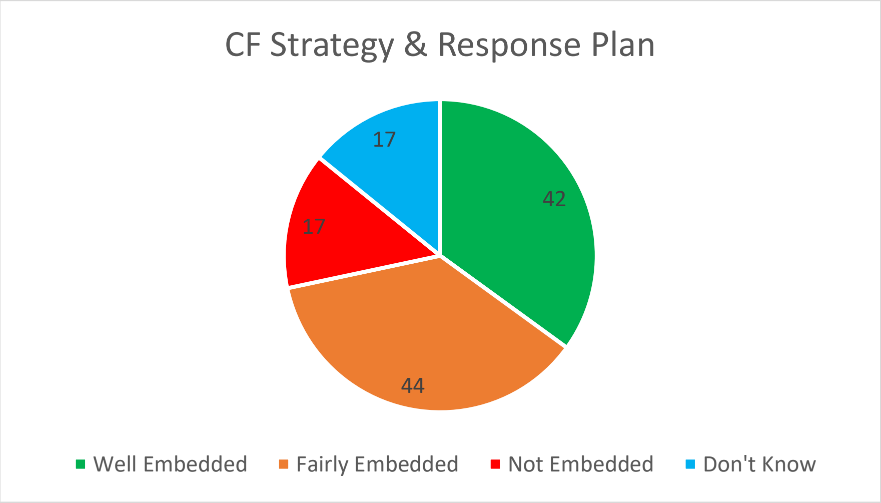
Covid 19 Business Grants

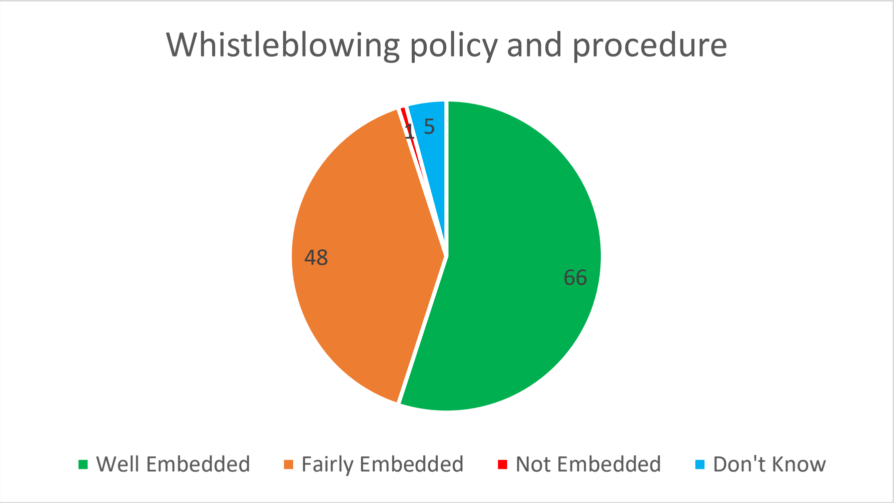
4.13 The Business Rates Section has been progressing the fraudulent cases through the recovery process in accordance with the Government’s Debt Recovery Guidance. This involves a three-step debt recovery process before a debt is referred to the Department for Business, Energy and Industrial Strategy for appropriate action.

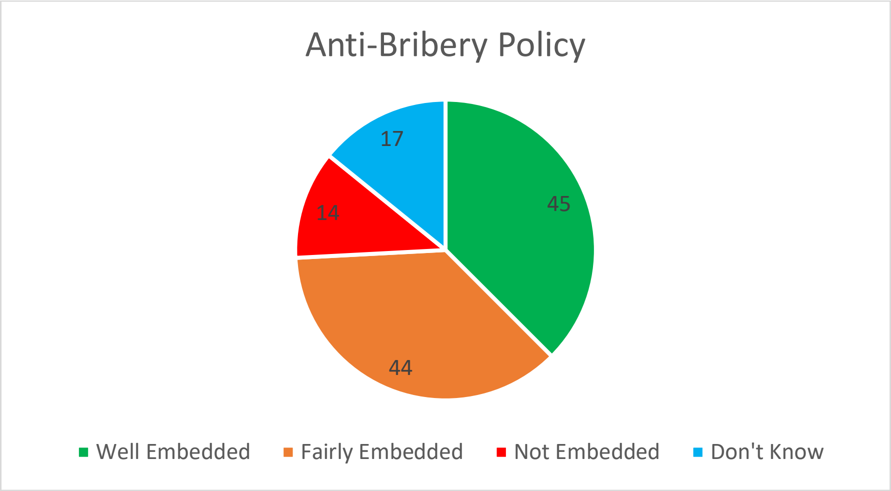
4.14 There are 28 cases that are being actively pursued by the Business Rates Section to the value of £277k. We have been advised that approximately 70% of the cases have had all the required action and are currently being reviewed for referral to the Department for Business, Energy, and Industrial Strategy as above.

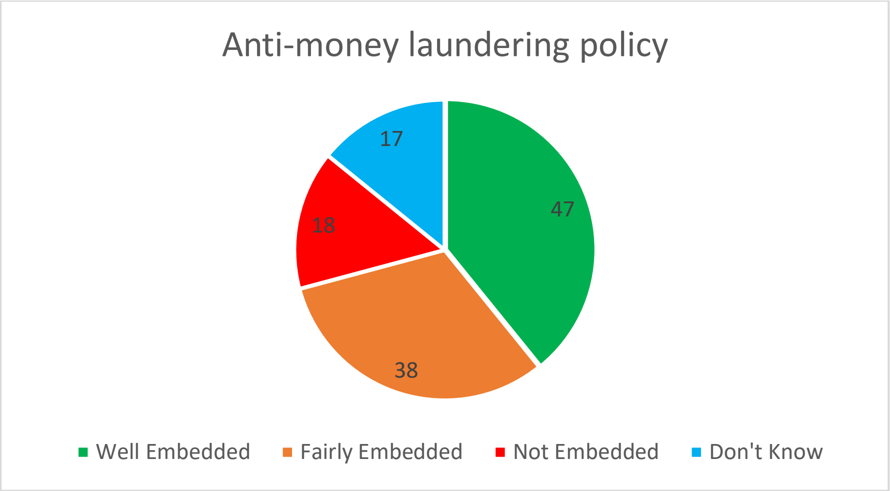
5 Survey of Internal Control

5.1 The Survey of Internal Control (SIC) is used to gain operational assurance as to whether systems of internal control are embedded and functioning. The survey asked Senior Managers about the Council’s approach to counter fraud and corruption including the Council’s Counter-fraud and Corruption Strategy and Response Plan, Whistleblowing Policy, Anti Bribery Policy and Anti Money Laundering Policy. The responses are shown below:









5.2 The results show that overall the suite of counter fraud policies are embedded across the organisation with the majority of respondents confirming the Whistleblowing arrangements are generally well embedded. This gives some assurance that staff are aware of the policy and how to report concerns of wrongdoing in the Council.

5.3 It has highlighted some areas where we can strengthen awareness of the arrangements which will be addressed through increased Directorate engagement, and efforts to promote the Fraud Awareness Training. At the time of reporting, we are reviewing the areas in which it is clear there are opportunities for further engagement to understand the root causes and risk posed. We will reflect on this and will review the impact of steps taken through future responses to the survey.

6 Regulation of Investigatory Powers Act 2000

6.1 In the most recent inspection report issued by the Office of Surveillance Commissioners, it was recommended that Members should receive regular reports about the use of the Council's surveillance powers under RIPA.

6.2 The Regulation of Investigatory Powers Act 2000 (RIPA) is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with when the law permits and there is a clear public interest justification.

6.3 RIPA provides an authorisation process for certain types of surveillance and information gathering, and that process can be used as a defence against human rights claims. At present, the Council is entitled to authorise its own directed surveillance and can also authorise the use or conduct of a CHIS (covert human intelligence source) under RIPA, and the Council's RIPA policy contains a number of safeguards against the over-use of these powers.

6.4 In addition, local authorities can only authorise directed surveillance for preventing or detecting "serious crime" which is defined as criminal offences punishable by at least 6 months imprisonment, or certain other specified offences, and the use of a CHIS can only be authorised for the purpose of preventing or detecting crime or of preventing disorder. RIPA also now specifies that a directed surveillance or CHIS authorisation cannot take effect until such time as a Justice of the Peace (JP) has made an order approving the authorisation.

6.5 In practice, the only Services who have used directed surveillance previously as part of their investigations have been those involved in combatting anti-social behaviour or dealing with environmental health issues. However, the Council's RIPA policy encourages the use of RIPA as a last resort only, and the "default position" in all Services now is to undertake investigations overtly. In addition, there is occasional use of directed surveillance in relation to the investigation of insurance claims, and by West Yorkshire Trading Standards. There has been only one directed surveillance authorisation (in relation to a Trading Standards matter) in the last 7 years, and no CHIS authorisations.

6.6 As described above, given the terms of the RIPA policy, and the Council's Values, the "default" position is that overt methods should be used in all but exceptional cases. In addition, the grounds for authorising surveillance are limited, and approval by a JP is now also required in all cases. Therefore, it seems unlikely that the Council's use of RIPA powers will increase.

6.7 In addition, given the Council is effectively a non-user of these powers, it would take quite a lot of resource to get the necessary arrangements in place if a Service wanted to start using these powers again. For example, staff in the relevant Service would need to be trained as applicants, and a minimum of 2 authorising officers at Head of Service level, would need to be re-trained in order to deal with directed surveillance authorisations, and costs would also be incurred in making applications to the Magistrates Court. Therefore, any Service which proposed to use these powers would need to be clear about why this was necessary, and how they would meet the costs of putting the necessary arrangements in place.

6.8 In relation to the acquisition of communications data, the Investigatory Powers Act 2016 now requires all local authorities to be party to a collaboration agreement. In practice this means becoming a member of National Anti-Fraud Network (NAFN) and using their Single Point of Contact (SPoC) service. However, these agreements have to be certified by the Secretary of State and are subject to review every 3 years. The NAFN SPoC would then scrutinise the Council's applications, and then applications would have to be submitted to the OCDA (Office for Communications Data Authorisations) for authorisation. There is also a limitation that if the data sought is wholly or partly "events data", in other words if it identifies or describes an event whether or not by reference to its location, then the Council's purpose would have to be preventing or detecting "serious crime", which is basically an offence which carries a prison sentence of at least 12 months.

6.9 The relevant Code of Practice says that in addition the SRO, or person of equivalent rank should be made aware of applications before they are submitted to the OCDA, and that the officer “verifying” the application are of “an appropriate rank”. Although it is a little unclear quite what the IPC expect by way of verification, and how this fits with the SPoC oversight, it can be assumed this means a senior manager would need to be nominated to carry out this role.

6.10 Therefore, before the Council could start to use these powers again, if not already a member the Council would need to join NAFN, enter into a collaboration agreement and get it certified by the Secretary of State, train a number of staff to be applicants, nominate and then train one or more senior managers so that they can verify applications, and get approval from the SRO and City Solicitor for these arrangements.

6.11 Given the amount of resource all of this would be likely to take, and the Council’s policy to use covert methods only when there is a clear case for saying overt methods will not suffice, a Service would need to be very clear about how they were proposing to use these powers over the life of the collaboration agreement, and how they would meet the costs of these arrangements.

6.12 Legal services have confirmed that there have been no applications for directed surveillance or covert human intelligence source (CHIS) authorisations since the previous update was provided (which covered the period to March 2023). In addition, there has been no use of the powers to obtain communications data over the same period.

Anti-Bribery Policy

Leeds
CITY COUNCIL

Reviewed and updated: February 2024
Next review due: 2027

Contents

1.0 INTRODUCTION

1.1 Leeds City Council is committed to the highest standards of integrity, honesty and openness, and expects the highest standards of conduct from its employees, contractors and elected Members. All employees, contractors and elected Members are expected to abide by their respective codes of conduct and act in accordance with the Council's values and behaviours to work collectively to achieve the objectives set out in the Best City Ambition.

1.2 Bribery is a criminal offence for which the Council has zero tolerance, and the Council is committed to the prevention, deterrence, and detection of bribery in all areas of their activities. The Council does not, and will not, pay bribes or offer improper inducements to anyone for any purpose, nor accept bribes or improper inducements. To use a third party as a conduit to channel bribes to others is a criminal offence and the Council does not, and will not, engage indirectly in or otherwise encourage bribery.

2.0 SCOPE OF THE POLICY

2.1 To help protect the Council against the offence of bribery it is important that everyone within 'Team Leeds' understands what offences constitute as bribery, the law surrounding this and the arrangements in place within the Council to mitigate the risk and enable compliance. In conjunction with related Council policies and key documents it will also enable the identification and effective reporting of a potential breach.

2.2 This policy will:

- Demonstrate the Council's commitment to tackling bribery and corruption.
- Make all staff aware of their responsibilities to adhere strictly to this policy at all times.
- Encourage everyone to be vigilant and provide details of how to report any suspicions of bribery.
- Offer reassurance that the Council will treat all allegations of bribery seriously and investigate as appropriate, assisting police and other appropriate authorities in any resultant prosecution.
- Confirm that the Council has a zero-tolerance stance and will take action against any individual(s) involved in bribery.

2.3 The responsibility to control the risk of bribery occurring resides at all levels of the Council and not solely within assurance functions. It is everyone's responsibility to be open, honest and trusted in line with the core values and expected behaviours of the Council, in line with the code of conduct. It is also imperative that we act with integrity, protect public funds and spend money wisely.

This policy applies to all staff (permanent, temporary, agency), contractors/suppliers, elected members (including independent members), volunteers and consultants and anyone associated with the Council.

3.0 WHAT IS BRIBERY?

3.1 Bribery is an inducement or reward offered, promised, or provided to gain personal, commercial, regulatory, or contractual advantage.

The Bribery Act 2010 (the "Act")

3.2 There are four key offences under the Act:

- bribery of another person – offer, promise, or give a bribe (section 1)
- accepting a bribe – request, agree to receive, or accept a bribe (section 2)
- bribing, planning to bribe a foreign public official – with the intention of obtaining or retaining business or an advantage in the conduct of business (section 6)
- failing to prevent bribery – corporate offence of failure by a commercial organisation to prevent bribery that is intended to obtain or retain business, or an advantage in the conduct of business, for the organisation (section 7)

3.3 An organisation will have a defence to failing to prevent bribery if it can show that it has in place adequate procedures designed to prevent bribery by, or of, persons associated with the organisation.

Other relevant legislation

3.4 The Criminal Finance Act 2017: This gives law enforcement agencies and partners, further capabilities, and powers to recover the proceeds of crime, tackle money laundering, tax evasion and corruption, and combat the financing of terrorism.

3.5 The Serious Crime Act 2015: The Serious Crime Act gives effect to a number of proposals set out in the Serious and Organised Crime Strategy. It builds on current criminal and civil law to ensure that the relevant bodies can effectively and relentlessly pursue, disrupt, and bring to justice serious and organised criminals.

4.0 Six principles of the Bribery Act

4.1 The procedures put in place by an organisation to prevent bribery should be informed by six principles.

4.2 Principle 1 - Proportionate procedures

Adequate procedures need to be applied proportionately, based on the level of risk of bribery in the organisation.
The Council has a range of policies and procedures in place which are proportionate to the level of risk it faces. The employee code of conduct and members codes of conduct set out the expected behaviours. These are supported by the gifts and hospitality policy and procedure and the employee outside interest policy. The council has a suite of counter fraud and corruption policies in place. This policy forms part of this framework along with the whistleblowing policy for reporting concerns of wrongdoing. The council has considered the risks posed in high-risk areas and has procedures in place to manage the risks. For example, as part of the procurement process.

4.3 Principle 2 - Top level commitment

The council fosters a culture in which bribery is never acceptable. The commitment by top level management is demonstrated through the endorsement of the counter fraud, bribery and corruption strategy and fraud awareness training (which includes bribery) by the Chief Executive. The chair of the corporate governance and audit committee is also the counter fraud champion who supports regular fraud and corruption communication.

4.4 Principle 3 - Risk Assessment

The Council assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it through risk management arrangements. Bribery is incorporated in the Fraud and Corruption risk of the Strategy and Resources risk register and is regularly reviewed. It includes financial risks but also other risks such as reputational damage.

4.5 Principle 4 - Due diligence

The council applies due diligence procedures where appropriate, taking a proportionate and risk-based approach, in respect of persons who perform or will perform services for or on behalf of the Council, to mitigate identified bribery risks. Due diligence forms part of the councils Contracts Procedure Rules. These set out the key responsibilities and actions staff must take when procuring goods or services to ensure a fair and transparent process for all.

4.6 Principle 5 – Communication (including training)

The Council seeks to raise awareness of the policies and procedures in place to prevent bribery and corruption through the fraud awareness training available on the Performance and Learning System (PALS). Regular internal communication also takes place. The Council’s stance on bribery and corruption is communicated externally on the council's website through the counter fraud and corruption strategy and fraud response plan.

4.7 Principle 6 - Monitoring and review

The Council monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.

5.0 PROSECUTION

5.1 The Director of Public Prosecutions and the Director of the Serious Fraud Office must give personal consent to a prosecution under the Act, as set out in section 10. These decisions are made in accordance with the Code for Crown Prosecutors.

5.2 Bribery is a serious offence and is an inherent public interest for this to be prosecuted to practically criminalise this behaviour.

5.3 Prosecution under the Bribery Act can be against both individuals and organisations if a person associated with it bribes another person, intending to obtain or retain business or an advantage in the conduct of business for that organisation. Penalties for individuals include unlimited fines and/or imprisonment and organisations can receive unlimited fines.

6. BRIBERY IS NOT TOLERATED

6.1 Bribery undermines democracy and the rule of law and improperly influences the decision-making process. It is important therefore that everyone is clear as to what is unacceptable.

6.2 It is unacceptable to:

- accept payment from a third party that you know, or suspect is offered with the expectation that it will obtain a business advantage for them or influence a decision.
- accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided by us in return or influence a decision.
- offer to influence a decision in return for a payment, gift or hospitality.
- retaliate against or threaten a person who has refused to commit a bribery offence or who has raised concerns under this policy.
- engage in any activity in breach of this policy.

7.0 WHAT ARE FACILITATION PAYMENTS?

7.1 A facilitation payment is a payment (money or goods) made to a public or government official that acts as an incentive for the official to complete some action or process expeditiously to the benefit of the party making the payment. In general, a facilitation payment is made to smooth the progress of a service to which the payer is legally entitled, without making such a payment.

7.2 These payments are not tolerated by the Council and are illegal under the Act.

8.0 GIFTS AND HOSPITALITY

8.1 This policy is not meant to change the requirements of the Employee Gifts & Hospitality Policy which forms part of the terms and conditions of employment with the Council.

8.2 The Employee Gifts & Hospitality Policy makes it clear that as an employee you should not benefit from your position at the Council beyond the pay and reward schemes that the Council has in place. The policy provides clear guidance regarding what is and what is not acceptable.

8.3 In summary never accept a gift or hospitality:

- As an inducement or reward for anything you do as an employee of the Council
- Which puts you under an improper obligation
- If acceptance might be open to misinterpretation

8.4 You must not solicit gifts or hospitality (other than modest refreshments which are incidental to the business at hand, for example a cup of tea at a meeting).

9.0 PUBLIC CONTRACTS AND FAILURE TO PREVENT BRIBERY

9.1 Under the Public Contracts Regulations 2015 where a contracting authority has knowledge that a company or its representatives have been convicted of a corruption offence, they should be treated as ineligible (debarred) to participate in the tendering process. Companies cannot be permanently debarred, but instead will face a term of debarment, dependent on the case, that can be no longer than five years from the date of the conviction.

9.2 Public authorities are also obliged to bring debarment to an end when the company can satisfactorily demonstrate ‘self-cleaning’. This allows companies to recover eligibility to bid for public contracts following a debarment by demonstrating sufficient evidence of the following:

- payment of, or undertaking to pay, compensation in respect of any damage caused by the criminal offence or misconduct.

- clarification of the facts and circumstances of the offence in a comprehensive manner, for example by actively collaborating with the investigating authorities
- the introduction of concrete technical, organisational and personnel measures, which are appropriate to prevent further criminal offences or misconduct.

10.0 STAFF RESPONSIBILITIES

10.1 The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for the Council or under its control. All appropriate staff are required to avoid activity that breaches this policy.

10.2 You must:

- ensure that you read, understand, and comply with this policy.
- raise concerns as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. Details of how to raise concerns can be found below in section 11.

10.3 As well as the possibility of civil and criminal prosecution, staff that breach this policy will face disciplinary action, which could result in dismissal for gross misconduct.

11.0 RAISING A CONCERN

11.1 We all have a responsibility to help detect, prevent, and report instances of bribery. If you have a concern regarding a suspected instance of bribery or corruption, please speak up – your information and assistance will help. The sooner you act, the sooner it can be resolved.

11.2 The Council is committed to ensuring that there is a safe, reliable, and confidential way of reporting suspicious activity and that staff know how they can raise concerns.

11.3 Concerns can be raised with your line manager or a senior manager within your service. You can raise your concern initially in person, by telephone or in writing. The manager will consider any information you provide in line with the requirements of this policy.

11.4 Concerns can be raised anonymously and will be considered wherever possible at the discretion of the Council. However, it may be more difficult or even impossible to investigate them properly if further information cannot be obtained from the informant. This policy encourages you to provide your name and contact details when reporting your concern.

11.5 If you would prefer to report your concerns directly to Internal Audit, or you are not a Council employee or worker, then a referral can be made as follows:

Telephone:	0113 378 8008 (dedicated hotline answered by a member of the Internal Audit team or an answerphone).
Email:	concerns@leeds.gov.uk
In writing:	Internal Audit, 3rd Floor West, Civic Hall, Leeds, LS1 1JF.
Online (internal only):	When logged into the Council network there is the option to complete a whistleblowing referral form via Insite.

11.6 The Council is committed to treating all concerns raised consistently and fairly. Where a referral is made to Internal Audit an initial assessment of the information received will be completed which may include preliminary enquiries. This will determine if further investigation will be undertaken and if so, who is best placed to complete this considering any skills, knowledge and areas of expertise felt to be necessary.

11.7 Details of all referrals received by managers under this policy should be notified to Internal Audit to allow a central record to be maintained. A regular review of referrals notified and actioned by management will be undertaken to ensure all concerns are being dealt with on a consistent basis.

11.8 The Council recognises that as a Council employee or worker, the decision to report a concern can be a difficult one to make, not least because of the fear of reprisal from those responsible for the wrongdoing. The Council will not tolerate harassment or victimisation and will take action to protect you when you raise a concern which you reasonably believe to be true.

11.9 If you have any questions about these procedures or need further advice, please contact internalaudit@leeds.gov.uk.

12.0 OTHER RELEVANT POLICIES

Members Code of Conduct
Employee Code of Conduct
Employee Gifts and Hospitality Policy
Employee outside interests’ policy and procedure
Anti-Money Laundering Policy & Policy on a page
Whistleblowing Policy
Counter fraud and corruption strategy

This page is intentionally left blank

WHAT IS BRIBERY?

Bribery is an inducement or reward offered, promised or provided to gain personal, commercial, regulatory or contractual advantage

Bribery is a form of corruption. **Corruption** can be defined as any unlawful or improper behaviour that seeks to gain an advantage through illegitimate means.

THE BRIBERY ACT 2010

Four key offences under the Act

① bribing another person (section 1)

② being bribed (section 2)

③ bribing a foreign public official (section 6)

④ failure by a commercial organisation to prevent bribery (section 7)

Bribery is a criminal offence and can result in imprisonment and/or unlimited fines for the individuals and organisations.

ANTI-BRIBERY POLICY

Sets out what bribery is, the law, the arrangements in place within the council to mitigate the risk and enable compliance by all council staff and its associates (for example, contractors). In conjunction with related council policies and key documents it will also enable the identification and effective reporting of a potential breach.

Bribery undermines democracy and the rule of law and improperly influences the decision-making process. Bribery will not be tolerated. As well as the possibility of civil and criminal prosecution, staff that breach this policy will face disciplinary action, which could result in dismissal for gross misconduct.

RESPONSIBILITIES FOR ALL

The responsibility to control the risk of bribery occurring resides at all levels of the Council and not solely within assurance functions. It is everyone's responsibility to be open, honest and trusted in line with the core values and expected behaviours of the Council, in line with the code of conduct. It is also imperative that we act with integrity, protect public funds and spend money wisely.

REPORTING CONCERNS

Concerns should be raised with management or Internal Audit. Details can be found in the anti-bribery policy. If you are a manager and receive a report of bribery, please inform Internal Audit of the details and how this has been addressed so we can monitor consistency in the councils response.

Whistleblowing hotline :
0113 3788008

Email:
concerns@leeds.gov.uk

Whistleblowing referral online form on Insite

For general advice contact
internalaudit@leeds.gov.uk

GUIDANCE AND TRAINING

Guidance around how to identify and address any concerns around bribery can be found in the Anti Bribery Policy.

The free fraud awareness training available on the PAL system is designed to raise awareness of fraud, bribery and corruption that could impact the council. The dedicated bribery and corruption module includes scenarios that should help you spot these, your responsibilities and how to report concerns.

Leeds
CITY COUNCIL

This page is intentionally left blank

Agenda Item 12

Leeds
CITY COUNCIL

Report author: Mary Hasnip

Tel: 3789384

Update report on Government Proposals to address the national audit backlog, and Grant Thornton's Response and update on the Audit 2021/22

Date: 19th February 2024

Report of: the Chief Finance Officer

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

Brief summary

This report informs Members of the Government's most recent proposals to address the backlog of incomplete audits across local government in England.

Grant Thornton's accompanying report sets out their intended approach in response to the Government's proposals, should these go ahead. The report also provides a summary update on the progress towards completing the audit of the 2021/22 statement of accounts.

Recommendations

a) Members are asked to note the information provided in this report on the Government's intention to introduce an audit backstop date, and to note Grant Thornton's proposed course of action for the 2022/23 audit and their progress towards completing the 2021/22 audit.

What is this report about?

1 This report outlines the latest information available on the Government's proposals to address the national backlog in local authority audits, the uncertainties that remain, and the potential implications for the Council's audit and accounts process.

2 The Government's intended approach to address the audit backlog has been published in a letter from the Minister for Local Government to the Chair of the Public Accounts Committee. The full text of the letter is attached as an appendix to Grant Thornton's report. The relevant paragraph of the Minister's letter reads :

> "Our proposals will include an initial backstop date for local authorities and auditors of 30 September 2024 for all outstanding local audits in England up to and including the financial year 2022/23. Subject to the outcome of the consultations on necessary legislative changes as well as changes to the Code of Audit Practice, we intend to bring forward legislation to implement the backstop proposals. While these consultations take place, preparers and auditors should continue undertaking existing work to produce and audit local authority financial statements to ensure the system is in the best place possible to implement any final package of measures."

3 No details are available yet on how the backstop would work, on what form of words might be used for an audit opinion if the backstop was applied, or on what the implications may be for future years' audits where the backstop has been applied.

4 The Council intends to respond to the Government's consultation once this is issued, and further updates will be provided to Members at future meetings of the Committee on the detail of the proposals. Given the need for a consultation and for legislation, whilst the backstop may be likely to happen, at this stage it is by no means certain that it will be introduced on the date currently intended.

5 Grant Thornton's report outlines their intended approach in response to the Government's backstop proposals, and also provides a summary update of progress on the 2021/22 audit.

6 As it is now expected that the Committee will be asked to approve the 2021/22 statement of accounts on behalf of the Council at the March meeting, an informal briefing session on the 2021/22 accounts will be arranged for Members in advance of that meeting.

What impact will this proposal have?

7 Grant Thornton's report explains that they propose to carry out the 2022/23 audit from April 2024, at a time when the council will be closing down the 2023/24 financial year and preparing its 2023/24 draft accounts. This will have implications for staffing resources within Financial Services. However it gives the best opportunity for completing the 2022/23 audit before the potential backstop date of 30th September 2024.

How does this proposal impact the three pillars of the Best City Ambition?

☐ Health and Wellbeing ☐ Inclusive Growth ☐ Zero Carbon

8 The report relates to the council's underlying financial governance arrangements rather than to any specific aspect of service delivery.

What consultation and engagement has taken place?

Wards affected:

Have ward members been consulted? ☐ Yes ☒ No

9 The audit report does not raise any issues requiring consultation or engagement with the public or ward members.

What are the resource implications?

10 There are implications for the level of staffing resources required if the 2022/23 audit is to be carried out at the same time as the 2023/24 closedown process and the ongoing project to introduce the new financial ledger. These implications are under consideration by the Chief Officer, Financial Services.

What are the key risks and how are they being managed?

11 There is a risk that, if the proposed backstop does go ahead, the Council's accounts for 2022/23 may not be subject to a full audit. Grant Thornton have put forward a proposed approach to manage this risk, and officers within Financial Services will do their best to support this approach.

What are the legal implications?

12 Subject to consultation responses, the Government proposes to introduce legislation which would introduce a backstop date of 30th September 2024 for incomplete local authority audits up to and including 2022/23.

Options, timescales and measuring success

What other options were considered?

13 The report provides information to Members on aspects of the audit process, and does not relate to a decision.

How will success be measured?

14 The delivery of final audited accounts for 2021/22 and 2022/23 would represent a successful outcome.

What is the timetable and who will be responsible for implementation?

15 The timing of the Government's consultation on its proposed backstop arrangements is not yet known.

16 Grant Thornton intend to present their final audit report on the 2021/22 accounts at the February meeting of the Committee.

Appendices

- Appendix 1 is Grant Thornton's report, entitled 'Audit Progress on 2021/22 Accounts Audit and Implications of Proposed 'Backstop' on the 2022/23 Accounts Audit'.

Background papers

- None

Agenda Item 13

Report author: Kate Sadler

Tel: 0113 37 88663

Corporate Governance and Audit Committee Work Programme 2023-24

Date: 12th February 2024

Report of: Chief Officer Financial Services

Report to: Corporate Governance and Audit Committee

Will the decision be open for call in? ☐ Yes ☒ No

Does the report contain confidential or exempt information? ☐ Yes ☒ No

Brief summary

This report presents the work programme for the Corporate Governance and Audit Committee, setting out future business for the Committee's agenda, together with details of when items will be presented.

Development and regular review of the work programme enables the Committee to manage the business appropriately in line with the risks currently facing the Council.

Recommendations

a) Members are requested to consider and approve the work programme and meeting dates at Appendix A.

What is this report about?

1 This report presents the work programme for the Corporate Governance and Audit Committee.

What impact will this proposal have?

2 The work undertaken by the committee throughout the year will support the understanding of the internal control and risk environment and support the committee's approval of the statutory Statement of Accounts and Annual Governance Statement (the AGS).

How does this proposal impact the three pillars of the Best City Ambition?

☒ Health and Wellbeing ☒ Inclusive Growth ☒ Zero Carbon

3 The work undertaken by the committee will provide assurance that arrangements for internal control support the delivery of the council's strategic objectives.

What consultation and engagement has taken place?

Wards affected:

Have ward members been consulted? ☐ Yes ☒ No

4 The work programme was approved by the Committee at its meeting in March 2023 and is presented at each meeting for the Committee to consider and amend as appropriate.

What are the resource implications?

5 The work undertaken by the committee will provide assurance as to the appropriate use of resources to deliver the council's strategic objectives.

What are the key risks and how are they being managed?

6 The work undertaken by the committee will provide assurance that there are arrangements in place for the management of risk which are appropriate, proportionate, monitored and effective.

What are the legal implications?

7 S151 Local Government Act 1972 requires local authorities to "make arrangements for the proper administration of its financial affairs". The Accounts and Audit (England) Regulations 2015 provide that the local authority is responsible for ensuring "a sound system of internal control which facilitates the effective exercise of its functions and the achievement of its aims and objectives; ensures that the financial and operational management of the authority is effective and includes effective arrangements for the management of risk".

8 The work undertaken by the Committee enables it to advise Council (the body charged with governance) that arrangements in place are up to date, fit for purpose, communicated, and embedded, monitored, and routinely complied with.

Options, timescales and measuring success.

What other options were considered?

9 Members are invited to recommend the inclusion of business in the 2024-25 work programme as necessary.

How will success be measured?

10 The Committee will provide an annual report to Council detailing how the committee has discharged its responsibilities.

What is the timetable and who will be responsible for implementation?

11 As set out at Appendix A.

Appendices

- Appendix A – Work Programme of Corporate Governance and Audit Committee 2023/24

Background papers

- None

Work Programme 2023/24

Date		Work Item	Author	Attendee	Category
26th **June** 2023	1	Internal Audit update report	Jonathan Foster	Angela Laycock	Internal Audit
	2	Counter Fraud and Corruption update report	Louise Ivens	Louise Ivens	Internal Audit
	3	Civica CX (Housing) and FMS (Finance) systems interfaces	Helen Jackson	Girish Solanki	Additional Assurance
	4	Draft annual report 2021/22 of CGAC to Council	Liz Gott	Kate Sadler	Effectiveness
24th **July** 2023	1	Internal Audit Annual report and opinion (including assurance in respect of RIPA)	Jonathan Foster	Angela Laycock Louise Ivens	Statutory
	2	Draft Statement of Accounts (for information)	Mary Hasnip	Mary Hasnip	Statutory
	3	Interim Annual Governance Statement (for information)	Kate Sadler	Kate Sadler	Statutory
	4	Grant Thornton Interim Audit Findings Report 2021-22		GT	External Audit
25th **September** 2023	1	Annual assurance report on planning regulation and enforcement arrangements	Helen Cerroti	David Feeney	Annual Assurance
	2	Annual assurance report on decision making	Liz Gott / Kate Sadler	Liz Gott / Kate Sadler	Annual Assurance
	3	Internal Audit update report	Jonathan Foster	Angela Laycock	Internal Audit
	4	Approval of Annual Governance Statement 2023	Kate Sadler	Kate Sadler	Statutory
	5	Work Programme	Kate Sadler	Liz Gott / Kate Sadler	

Date		Work Item	Author	Attendee	Category
27th **November** 2023	1	Annual assurance report on procurement policies and practices	Kieron Dennett / Lewis Sinkala	Kieron Dennett / Lewis Sinkala	Annual Assurance
	2	Annual assurance report on corporate performance management arrangements	Claire Keightley and Emma Kamillo-Price	Mike Eakins, Claire Keightley, and Emma Kamillo-Price	Annual Assurance
	3	Annual assurance report on corporate risk and resilience arrangements	Tim Rollett and Leanne Cummings	Tim Rollett and Leanne Cummings	Annual Assurance
	4	Annual report on financial planning and management arrangements (to include Treasury Management)	Richard Ellis	Richard Ellis	Annual Assurance
	5	Receipt of External Auditor's IT Audit Report 22-23	Mary Hasnip	GT	External Audit
	6	Receipt of External Auditor's Annual Report including Value for Money Findings 22-23	Mary Hasnip	GT	External Audit
	7	Receipt of External Auditor's ISA 260 Update Report 21-22	Mary Hasnip	GT	External Audit
	8	Work Programme	Liz Gott / Kate Sadler	Kate Sadler	
12th February 2024	1	Update report on Information and Digital Services Governance	Andrew Byrom	Leonardo Tantari	Annual Assurance
	2	Joint Annual Report on Information Governance from the Data Protection Officer and Caldicott Guardian.	Aaron Lindon / Shona McFarlane	Aaron Lindon / Shona McFarlane.	Annual Assurance

Date		**Work Item**	**Author**	**Attendee**	**Category**
	3	Internal Audit update report	Jonathan Foster	Angela Laycock	Internal Audit
	4	Counter Fraud and Corruption update report (inc. RIPA)	Jonathan Foster	Jonathan Foster	Internal Audit
	5	Grant Thornton – Audit Update Report	GT	GT	External Assurance
	5	Work Programme	Liz Gott / Kate Sadler	Kate Sadler	
18th **March** 2024	1	Receipt of Internal Audit Plan	Jonathan Foster	Angela Laycock	Internal Audit
	2	Annual assurance report on employment policies and procedures and employee conduct	Claire Matson	Andy Dodman	Annual Assurance
	3	Receipt and approval of Audited Accounts and External Auditors Audit Report for 2021-22.	Mary Hasnip	Mary Hasnip and GT	Statutory External Audit
	4	Proposed Work Programme	Kate Sadler	Kate Sadler	Effectiveness

This page is intentionally left blank