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

Effectively Embed

4. Statutory and non-statutory information requests

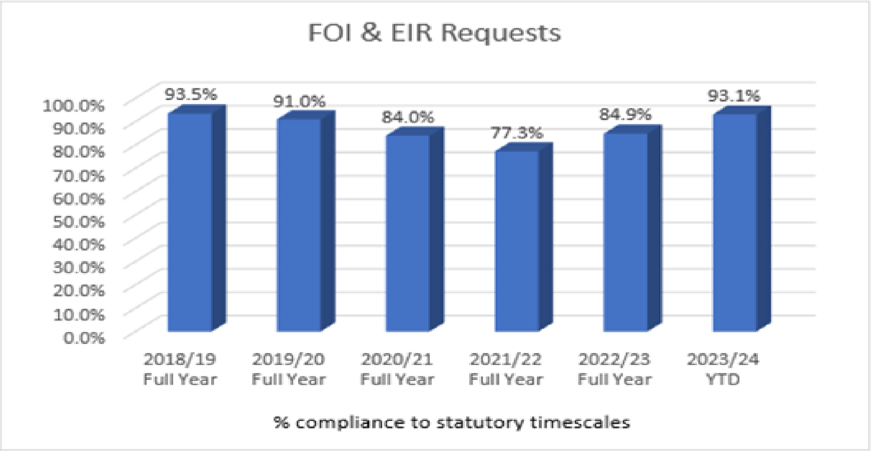
4.1. Data protection law gives individuals greater control over their personal data through several rights. Individuals are informed of their rights through the Leeds City Council Privacy notice available on our website. All staff are made aware of these rights through the information governance e-learning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

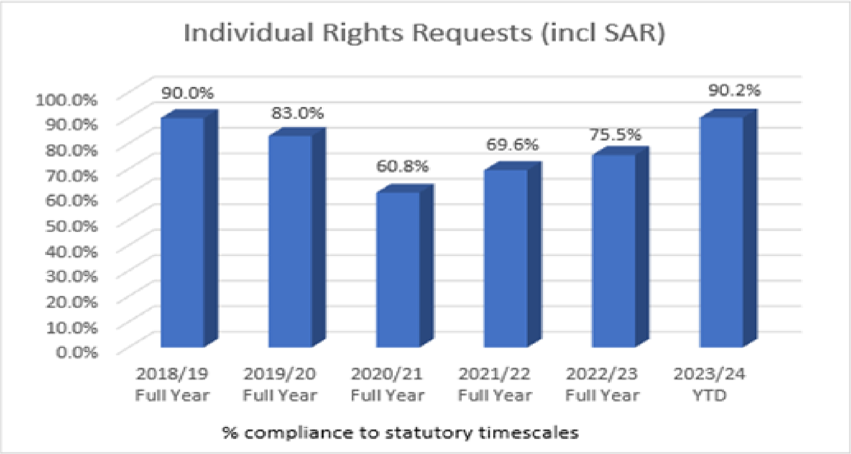
4.2. The IM&G service is responsible for processing and responding to all information requests to the council. This includes those made under the Freedom of Information Act 2000 (FOIAs) and the Environmental Information Regulations 2004 (EIRs), the UK General Data Protection Regulation (GDPR) (Individual 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.

Meaningfully Monitor

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.