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.

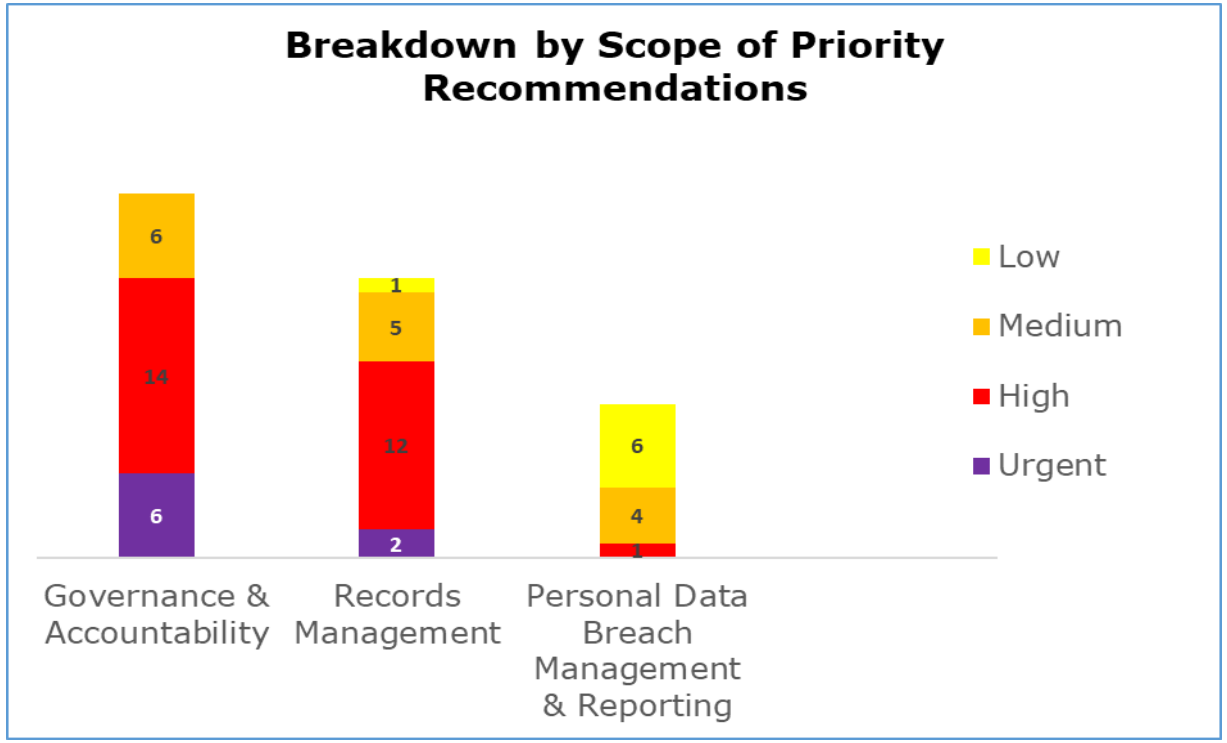
Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, both on-site and remote interviews with selected staff, an inspection of selected records and a virtual review of evidential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

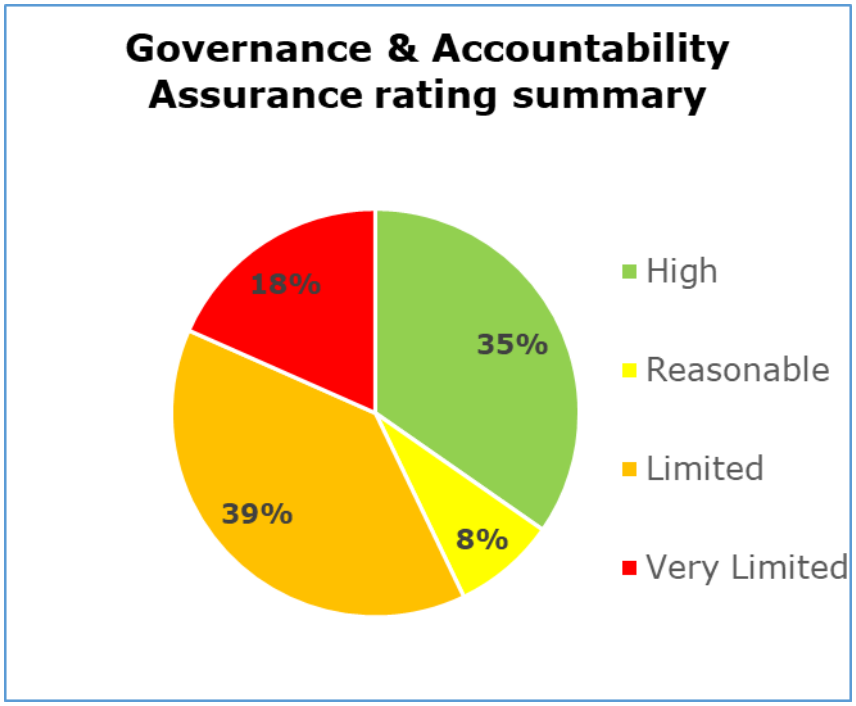
Priority Recommendations



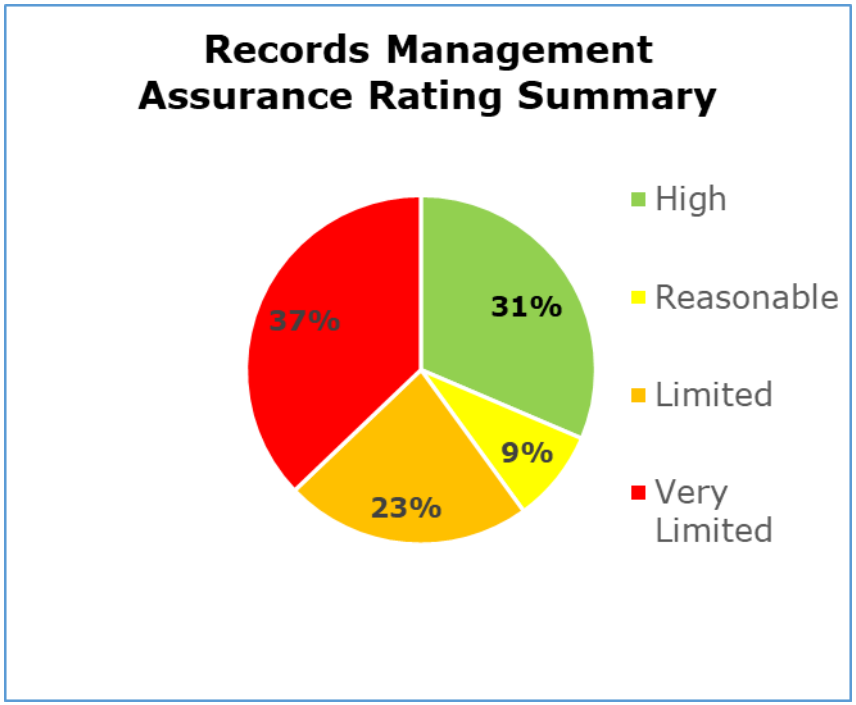
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- 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.

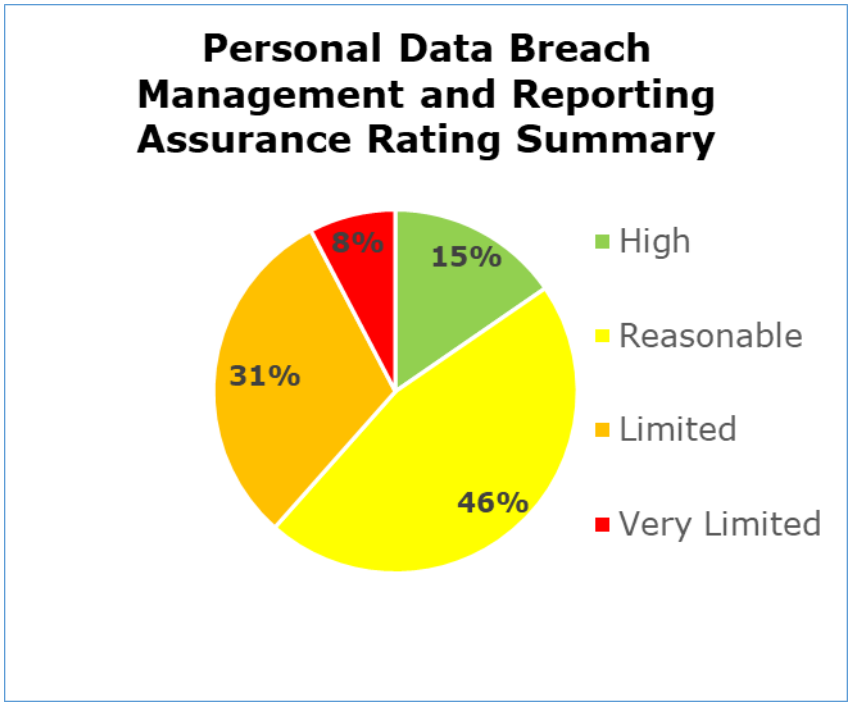
Graphs and Charts



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:

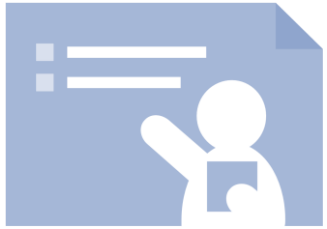
- LCC must complete an information audit and use it to inform their information asset register (IAR), RoPA and a weeding schedule and guidance. Without this, they cannot be assured they have full visibility of their information assets or the data quality of the assets.
- Disposal of excessive records 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

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

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

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

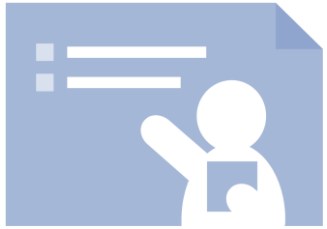
The tables below list observations made by auditors during the course of the audit along with suggestions to assist LCC with possible changes.

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.

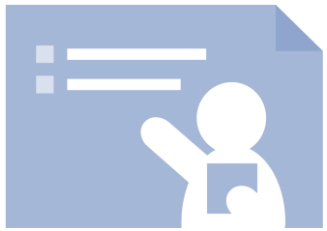
Appendices



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.