

Lincolnshire County Council

Data protection audit report

January 2025

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.

Lincolnshire County Council (LCC) agreed to a consensual audit of its data protection practices.

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 areas:

Scope area	Description
Governance & 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 LCC.
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.
Training & Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

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, remote interviews with selected staff, and a virtual review of evidential documentation.

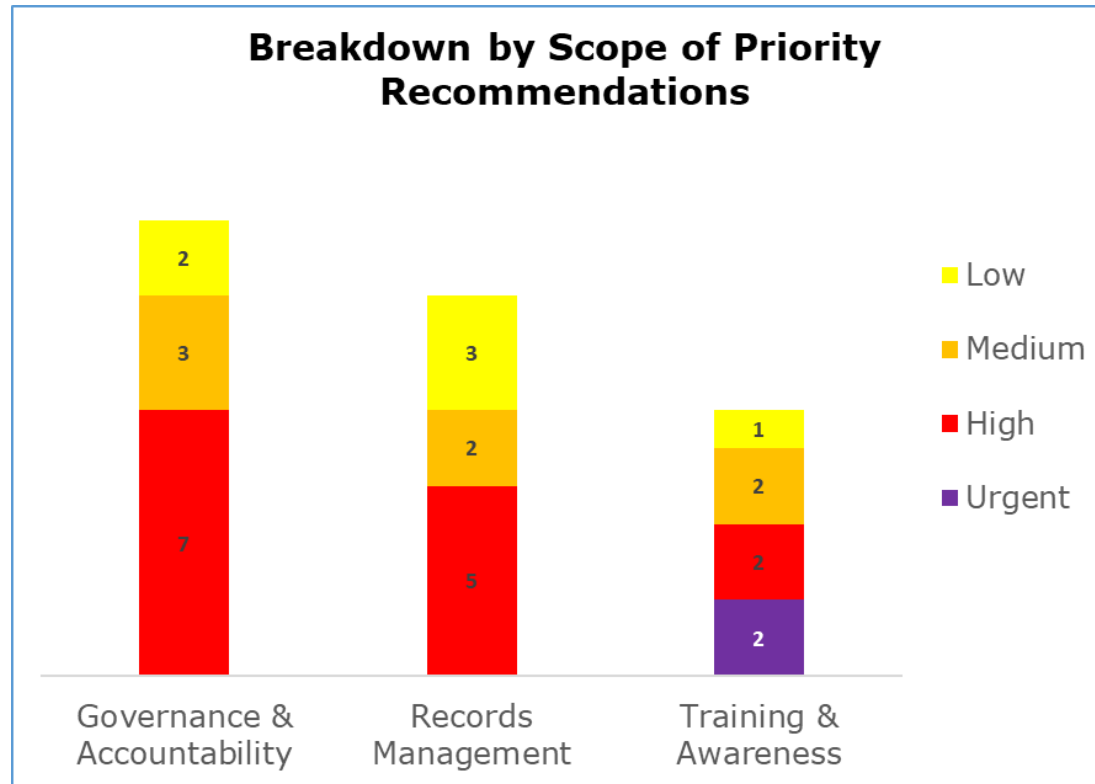
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LCC in implementing the recommendations each has been assigned a priority rating based upon the risks that they 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 & 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	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.
Training & Awareness	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.

*The assurance ratings are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

Priority Recommendations



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

- Governance & Accountability has no urgent, seven high, three medium and two low priority recommendations.
- Records Management has no urgent, five high, two medium and three low priority recommendations.
- Training & Awareness has two urgent, two high, two medium and one low priority recommendations.

Key areas for improvement

Governance & Accountability

- LCC must document which records constitute the Council's record of processing activities (ROPA) and that the ROPA meets all relevant requirements set out in Article 30 of the UK GDPR.
- LCC should continue to enhance its data processor audit and compliance check programme to gain assurance data processors are adhering to all contract terms and conditions, and that logs are complete.
- LCC should revisit personal data breach trends and risk mitigation strategies to determine if further measures can be taken to minimise the risk of future personal data breaches.

Records Management

- LCC must continue with its established records management work programme to appraise and consolidate personal data held in physical format across its whole estate.
- LCC must take forward its defined strategy to appraise and consolidate personal data held in all its digital environments.
- LCC must adopt measures to manage retention in all digital environments where personal data is processed.

Training & Awareness

- LCC must ensure that individuals in specialised roles, such as those who are collecting personal data, receive specific training relevant to their role.
- LCC should implement measures to gain assurance that individuals who do not have access to the eLearning course have read and understood the provided material.
- LCC must ensure that if training is not completed either during induction or as part of the annual refresher training, access to personal data is either not granted or is revoked as appropriate.

Key areas of assurance

At the time of the audit and based on the evidence seen by ICO auditors, measures were in place and implemented effectively to meet the control objectives in the following key areas.

Governance & Accountability

- ICO auditors found evidence of a strong and knowledgeable information assurance team that adopts an innovative and iterative approach to data protection, effectively meeting the needs of LCC and data protection legislation.
- LCC have an effective Senior Information Risk Owner who champions information assurance in the Corporate Leadership Team and across the Council.
- LCC have appointed Information Asset Owners (IAOs) for all its information. These IAOs receive tailored and proactive updates. Furthermore, ICO auditors found that they have a good understanding of their responsibilities and actively fulfil the requirements of their role. This was found in relation to Governance & Accountability and Records Management scopes.
- LCC have effective mechanisms for recording, monitoring and reporting the work of the information assurance team, and this is used to inform key stakeholders. ICO auditors also found the information asset register (IAR) is integrated into the Council's processes and records, helping the Council maintain a consistent and comprehensive approach to data protection.
- The information assurance team demonstrated a strong understanding of the lawful bases for processing. ICO auditors found that where LCC relies on consent for processing personal data, it is effectively implemented and in accordance with Article 7 of the UK GDPR.

Records Management

- LCC has thoroughly assessed its risks to records management and proactively works to mitigate these through defined strategies and work programmes. It has made considered appropriate risk prioritisation.

- LCC has aligned its IAR to its records management strategy. The register is kept under proactive review to support ongoing accuracy.
- LCC have effective file retrieval systems in place.

Training & Awareness

- ICO auditors found a good awareness of information assurance, with its importance being supported throughout all areas of the Council.
- Staff at the LCC found that the awareness materials they are provided with are attention grabbing, engaging and easy to understand.
- LCC has a structure in place for regularly improving the training they provide, incorporating feedback from staff and piloting new training materials.

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 Lincolnshire County 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 Lincolnshire County Council. The scope areas and controls covered by the audit have been tailored to Lincolnshire County Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.