North West Leicestershire District Council

SENIOR INFORMATION RISK OWNER

REPORT 2024-25

Issued: 1 April 2025

1. Introduction

Within the Council the responsibility for good information risk management sits with all staff at all levels.

The Council’s Senior Information Risk Owner (SIRO) oversees information risk management and ensures regulatory compliance. The Council’s SIRO is the Head of Legal and Support Services.

The work of the SIRO is delivered through the Information Governance Team, which is led by the Council’s Data Protection Officer.

The responsibilities of the SIRO are as follows:

- To be accountable for risk management in relation to information governance at the Council;
- To take overall ownership of the Council’s information risk approach, including the information governance framework; and
- To oversee the information security incident procedure and the Council’s compliance in relation to dealing with information security incidents (data breaches).

The SIRO meets with the Information Governance Team on a quarterly basis to:

- Review compliance in relation to responding to requests for information and identify any areas of concern/potential risk;
- Identify whether any organisational or technical measures are required to address any risks presented by information security incidents that have occurred;
- oversee compliance on the completion and review of data privacy impact assessments;
- Identify and keep under review any potential projects that may involve data protection compliance; and
- Keep under review the Council’s Information Governance Framework and have regard to any changes that may be required as a consequence of any changes in legislation or guidance, or for any other reason.

2. Purpose of the Report

The purpose of this report is to provide an overview of the Council's compliance in relation to regulatory requirements and to set out how information risk has been managed across the organisation over the past year. It demonstrates how the Council has continued to meet its statutory regulatory requirements relating to the processing of personal data under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as well its duty to be transparent through compliance within the Freedom of Information Act 2000. The content of this report may vary from year to year depending on the activities undertaken and may include an overview of:

- Key achievements;
- Performance related to information governance;
- Compliance with statutory deadlines;
- Management of information security incidents;
- Compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR);
- Training and awareness

In addition, the report may also include policy and procedure updates; and the setting of objectives for the upcoming year.

3. Information Requests

Members of the public can request information from the Council under the Freedom of Information Act 2000 (FOIA) and/or the Environmental Information Regulations 2004 (EIR). The Environmental Information Regulations 2004 apply to all information which relates to the environment, in its broadest sense, including land, air, water, soil, buildings, animals and people, pollution of all kinds, waste, health and safety. This also includes reports, measures and analysis of environmental information. Whereas the FOIA applies to all other information. There are statutory deadlines by which the Council must respond to these requests for information. Under the legislation, the Council can apply exemptions where it is appropriate to do so to protect the information from disclosure e.g. confidential information. Each exemption has certain criteria that must be met before it can be applied and in some cases, the Council is required to consider a public interest test. The Council reports quarterly to its Audit and Governance Committee on how it is performing in relation to responding to information requests on time.

The following table sets out the number of requests received and responded to within the period 1 April 2024 - 31 March 2025:

2024/25	**Q1**	**Q2**	**Q3**	**Q4**	**TOTAL**
Total Number (FOIs)	122	132	197	204	655
% answered on time	89%	90%	92%	90%	90%
Average per month	39	44	65	68	54 (Av. Per Quarter)
Average response time (days)	11	14	9	8	11
Withheld due to exemption/fees	18	13	17	8	56
Transfers (TFRs)	22	27	16	24	89
Internal Reviews	0	0	2	2	4
Environmental Information Requests	4	6	1	6	17

The following table sets out the number of requests received and responded to within the period 1 April 2023 - 31 March 2024:

2023/24	**Q1**	**Q2**	**Q3**	**Q4**	**TOTAL**
Total Number (FOIs)	157	196	157	190	700
% answered on time	93%	86%	92%	92%	90%
Average per month	52	71	52	63	60
Average response time (days)	11	12	10	10	11
Withheld due to exemption/fees	13	2	13	19	47
Transfers (TFRs)	18	15	20	37	90
Internal Reviews	1	2	1	0	4
Environmental Information Requests	6	7	2	3	18

From the above figures it can be noted that:

- There has been a slight decrease in the number of requests that have been received under the FOIA & EIR for the period 1 April 2024- 31 March 2025.
- The average number of requests has increased each quarter for the period 1 April 2024- 31 March 2025.
- There has been an increase in the number of exemptions applied for the period 1 April 2024- 31 March 2025.
- The Council has maintained the target of 90% for the number of requests responded to on time.

The following table shows the number of requests received by service area within the period 1 April 2024-31 March 2025. This table includes requests made under the Freedom of Information Act and Environmental Information Regulation:

Service Area	**No. Requests**	**% of Total**
Communications	3	≤ 1%
Community Safety	17	2%
Corporate Leadership Team	1	≤1%
Customer Experience	3	≤1%
Customer Services	5	1%
Democratic Services	10	1%
Economic Development & Regeneration	6	≤1%
Environmental Health	23	3%
Environmental Protection	31	4%
Finance	55	8%
Housing Repairs	7	1%
Housing	70	10%
Human Resources	25	4%
ICT	20	3%
Legal Services	13	2%
Leisure Services	15	2%
Licensing	18	3%
Planning & Development	37	5%
Planning Policy	18	3%
Property Services	27	4%
Revenues & Benefits	45	6%
Waste Services	18	3%
Multiple Departments	19	2%

The following table shows the number of requests received by service area within the period 1 April 2023-31 March 2024:

Service Area	No. Requests	% of Total
Housing Team/Repairs	74	14%
Environmental Protection	69	13%
Planning & Development/Planning Policy	63	12%
Human Resources	55	10%
Finance	39	7%
Licensing	30	6%
ICT	30	6%
Waste Services	26	5%
Environmental Health	24	4%
Property Services	24	4%
Revenue & Benefits	24	4%
Environmental Health	22	4%
Leisure Services	20	4%
Democratic Services	18	3%
Economic Development & Regeneration	11	2%
Communications	9	2%

From the above figures it can be noted that:

- The Housing Service has received the highest number of requests for 2023/24 and 2024/25. It is believed that due to the nature of the work of the Housing Team, being customer facing, and the media interest within the Housing sector continues to generate housing related requests.
- The Planning Service has also maintained a higher proportion of requests compared to other service areas. This is believed to be due to the public interest in proposed new developments at a more local level, and an interest within Local Authority Planning Services at a wider level.

In addition to making requests for public information, individuals can also make a request to the Council for personal data held on them (subject access requests). The following table shows the number of subject access requests received in the period 1 April 2024 – 31 March 2025:

2024/25	Q1	Q2	Q3	Q4	TOTAL
Subject Access Requests (SARS)	11	10	12	21	54

This compares with the following in the previous financial year (2023/24)

2023/24	Q1	Q2	Q3	Q4	TOTAL
Subject Access Requests (SARS)	11	11	9	7	37

From the above figures it can be noted that:

- There has been an increase in the number of subject access requests received in the period 1 April 2024 to 31 March 2025.
- The quarterly figure remains consistent, with an increase in the number of subject access requests received in Q4 24/25.
- The Information Governance Team has not identified any particular trends; however, it is noted that there has been an increase in the number of subject access requests received in addition to individuals filing Housing disrepair claims.

4. Information Security Incidents

An information security incident (data breach) is a security risk which can result in the accidental or unlawful loss, destruction or disclosure of information. There have been 28 information security incidents reported during the period of 1 April 2024 – 31 March 2025. Each security incident has been investigated by the Data Protection Officer and where appropriate, measures and mitigations have been made to prevent the reoccurrence of similar incidents.

This represents an increase from the 15 information security incidents reported the previous year. Whilst this may indicate that Data Protection compliance has decreased, it is thought that with the implementation of the Data Breach and Information Security Procedure and training provided to staff through the Corporate Governance Training in November 2024, this has increased staff awareness of the duty to report suspected or actual information security incidents. It is really important that staff feel able to report suspected data breaches, so that they can be fully investigated and actions put in place to mitigate the risks.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

Personal data breaches can be categorised into:

- Confidentiality breach, where there is an unauthorised or accidental disclosure of, or access to personal data
- Availability breach, where there is a or loss of access to or destruction of personal data
- Integrity breach, where there is unauthorised or accidental alteration of personal data

The main incident type recorded was classified as a ‘Confidentiality Breach’. The majority of incidents reported related to personal data being disclosed to the incorrect recipient, mainly through email or letter.

The Information Governance Team is looking to enhance the reporting of data breaches to further categorise the nature of the breach, for example, email sent to incorrect recipient, unauthorised access to systems.

There have been two data breaches during this period that met the threshold to be reported to the Information Commissioner’s Office (ICO). The incidents included correspondence being disclosed to the wrong recipient. The incidents were investigated in line with the Councils Data Breach and Information Security Procedure and assessed against the risk matrix. It was deemed that the risk to the rights and freedoms of the individuals met the threshold for reporting to the ICO. In both cases immediate mitigations were implemented to reduce the risk to the affected individuals. Further recommendations were made to the relevant service areas to reduce the risk of similar occurrences happening in the future.

The Commissioner has provided a response in relation to both incidents to advise that the cases have been closed.

Whilst it is appreciated that there will be an element of human error, the Council has taken the following measures to reduce the likelihood of information security incidents occurring:

- Training provided to employees through the Corporate Governance Training Programme
- An updated online mandatory training course launched 1 April 2025
- Site audits commenced January 2025 across Whitwick Business Centre, Customer Services Centre and the Waste Services Depot to ensure Data Protection compliance
- Exploration of Microsoft Office functions to utilise available software to reduce information security incidents, for example, email classifications
- Quarterly meetings between the Data Protection Officer, ICT Manager and Audit Manager to discuss and address any security risks. Feedback will be provided to the Monitoring Officer at the quarterly SIRO meetings.

5. Organisational Compliance with Regulatory Requirements

Changes to Legislation in 2024/25

Whilst it was anticipated that a new Data Protection and Digital Information Bill would be introduced, this did not complete before parliament was dissolved on the 24 May 2024.

Following the formation of the new government, the Data Use and Access Bill (DUAB) was introduced to parliament in October 2024. The DUAB completed passage through the House of Lords in February 2025 and is expected to come into force at the end of 2025. The Information Governance Team is keeping this under review and will seek to implement any necessary changes should the DUAB be implemented.

Data Protection Impact Assessments

The Council manages a variety of personal information that is essential for service delivery. The Council has a statutory requirement to ensure that its information systems and supporting processes meet security, confidentiality, data protection and data quality needs. When implementing new policy and/or practical changes to the way in which personal data is processed, the Council carries out Data Protection Impact Assessments. This is to ensure any risks to privacy are mitigated and ensure that measures are in place to appropriately protect personal data.

During the period 1 April 2024 – 31 March 2025 there were 10 Data Protection Assessments carried out. This figure has increased from last year. Training has been provided through the Corporate Governance Training, which included the need for

Data Protection Impact Assessments to be carried out in relation to new and existing systems, where applicable. It is mandatory for a Data Impact Assessment to be conducted where it is deemed the processing of personal data is 'high risk'. The Council have introduced a Data Protection impact Assessment template, which includes an initial screening process. This will be assessed by the Data Protection Officer to determine if a full Data Protetion Impact Assessment is required. It is also considered even if processing is not deemed as 'high risk', as a Data Protection Impact Assessment is a useful tool when implementing change. This also demonstrates the Council's commitment compliance and accountability.

Data Protection Impact Assessments are kept under review to ensure that the measures remain appropriate.

Training and Compliance

Information governance training is mandatory for all officers including temporary and agency staff. It is carried out annually by all staff via an online platform and the target for completion is 100%.

During the period 1 April 2024- 31 March 2025, the completion rate is 86%.
As mentioned earlier in the report, the training programme for 2025/26 was launched on the 1 April 2025. The programme has been significantly updated to ensure that it is fit for purpose and covers all the required areas that staff need to be trained on. To improve and monitor compliance, going forward staff will be expected to complete the training within the month of April. If there are staff members who have not completed the training within the month of April, this will be addressed as appropriate.

In addition to the mandatory annual training, training on data protection was delivered by the Information Governance Team to the Council's Leadership Team and team managers as part of the Council's Corporate Governance training this year.

In the upcoming year, it is intended that more focused sessions will be provided in relation to FOI, EIR and Data Protection requests, where required.

Artificial Intelligence (A.I)

It is recognised that AI is being integrated into local government. The Council is currently looking at different AI products including Microsoft Copilot.

Whilst there are many organisational benefits to using AI, the Council will need to consider the risks that using AI technology poses.

The Information Governance Team will be working closely with the Council's Transformation Officer and relevant service areas looking to explore AI technology in order to ensure the Council remains complaint with its Data Protection responsibilities.

Policies

The Information Governance Framework has four policies that sets out the Council's approach to information governance. The policies were approved by Cabinet on the 24 September 2024, after having been presented to the Audit and Governance Committee on 7 August 2024. The policies included in the framework are:

- The Data Protection Policy
- The Information Security Policy
- The Information Rights Policy
- The Records Management Policy

The Information Governance Team has also created the following procedure documents to form part of the Information Governance Toolkit:

- Procedure for Information Sharing
- Information Requests Procedure
- Information Classification Procedure

The policies and procedures will be kept under regular review by the Information Governance Team.

ICT Security

The ICT Manager has confirmed that the following ICT security measures are in place for protecting the organisation:

- An annual IT security health check is conducted by an external Information Assurance for Small and Medium Enterprises (IASM) organisation. Any critical, medium, and high risks are resolved. The IT security health check is an assessment of the Council's security posture, where the internal and external network is check for vulnerabilities, to ensure that best practice is being followed, systems and applications have been patched and updated as well as overall security health of the Council's IT arrangements.
- Internal and external penetration testing is carried out, by a IASM security accredited supplier, with a remediation action plan in place to resolve any risks found. In 2024, the Council had no critical, six high, three medium and 23 Low issues. The high and medium issues have now been remediated. The Council has also passed its Public Sector Network (PSN) accreditation for 2024/25. The PSN accreditation, provides assurance to the Cabinet Office that the Council has maintained compliance for connecting to government networks.
- Phishing campaigns are conducted twice a year to test staff security awareness and feedback results to Corporate Leadership Team, with improvement plans in place for those who have not passed the test. Future campaigns will now include members as they were excluded previously.

- Quarterly Cyber Security awareness training is held for staff, members, and new starters, to protect staff at home and in the office. The completion rate is not as high as we would like it to be, and other ways to improve the uptake of this training are being explored. Annual mandatory cyber security training is also undertaken and this completion rate for this in 2024 was 85%
- New business systems are run in remote fully resilient data centres and existing systems are being progressively migrated to cloud computing or software as a service (SaaS) models, aligned to the ICT strategy of cloud first approach.
- Improved business recovery arrangements have been implemented to minimise recovery time. Accreditation to Cyber Essentials and the PSN has been secured.
- All of the the remediation recommendations arising from recent internal audits have now been completed successfully. Some formalisations of processes were required and these have been completed. An external vulnerability scanner has been purchased which allows the Council to scan and monitor the external perimeter daily and proactively mitigate issues. The latest scan showed 23 medium and 102 Low Vulnerabilities, which the Council is working to mitigate using the tool that has been purchased.
- Council backups have now been migrated to the cloud, with daily backups now stored off site. This has improved the Council's backup strategy and recovery times. The Council now has the ability to restore and recover back up files quickly, directly from the cloud, as opposed to using tapes, which took a long time to restore and can be unreliable
- Results of IT Health Checks are now reported to the Audit and Governance Committee. The IT Manager attended the last meeting to provide a update on the IT Health Check.
- The Council has completed the Cyber Assessment Framework (CAF) readiness program and is now working through the assurance piece of work with the Cabinet Office. This will ensure the Council is above the mandatory requirement for the completion of the CAF, when it is introduced into public and private sector organisations.