Appendix 1

North West Leicestershire
District Council

SENIOR INFORMATION RISK OWNER REPORT 2023-24

Issued: 2 April 2024

1. Introduction

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

The Council has appointed a Senior Information Risk Owner ("SIRO") to oversee its information risk management and ensure regulatory compliance. The Council's SIRO is the Head of Legal & 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'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;
- An overview of performance related to information governance;
- Compliance with statutory deadlines;
- Management of information security incidents;
- The Council's 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);
- Overview of training and awareness;
- Policy and procedure updates; and
- 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 is able to 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 to its Audit and Governance Committee quarterly 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 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 (FOI and BAU)*	13	2	13	19	47
Transfers (TFRs)	18	15	20	37	90

Internal Reviews	1	2	1	0	4
Environmental Information Requests/ Land Charges Searches (personal)	6	7	2	3	18

The following table shows the number of requests received per service area for requests made under the FOIA and EIR within the period 1 April 2023 – 31 March 2024. This information has been collated manually this year but it is hoped that in future years the system for logging requests will be able to generate the information.

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%

In the previous year (2022/23) the number of requests responded to was as follows:

2022/23	**Q1**	**Q2**	**Q3**	**Q4**	**TOTAL**
Total Number (FOIs)	147	122	108	148	525

% answered on time	51%	79%	60%	91%	71%
Average per month	49	41	38	49	44
Average response time (days)	7	9	14	13	11
Withheld due to exemption/fees (FOI and BAU)*	0	0	7	3	10
Transfers (TFRs)	29	21	18	26	94
Subject access requests (SARs)	3	6	5	10	24
Internal Reviews	1	3	3	1	8
Environmental Information Requests/ Land Charges Searches (personal)	4	4	7	7	22

From the above figures it can be noted that:

- Overall, there has been an increase in the number of requests received by the Council this year;
- Housing, Environmental Protection, Planning, Human Resources and Finance received the most requests this year;
- The percentage responded to on time each quarter has improved significantly this year;
- In more cases, the Council has had to apply exemptions to withhold information due to the nature of information being requested.

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 2023 – 31 March 2024:

2023/24	**Q1**	**Q2**	**Q3**	**Q4**	**TOTAL**
Subject access requests (SARs)	11	11	9	7	37

This compares with the following in the previous year (2022/23):

2022/23	**Q1**	**Q2**	**Q3**	**Q4**	**TOTAL**
Subject access requests (SARs)	3	6	5	10	24

From the above figures it can be noted that:

- Compared to last year, there has been an increase in requests received each quarter and overall across the year; and
- The number of subject access requests each quarter has remained consistent.

The Council has not identified any particular trends in subject access requests and is required to deal with any requests that are made.

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 15 information security incidents reported during the period of 1 April 2023 – 31 March 2024. Each security incident has been fully investigated by the Data Protection Officer and where appropriate, measures and mitigations have been made to prevent the reoccurrence of similar incidents.

The majority of the incidents reported this year were emails being sent to the wrong recipient. Whilst it is difficult to account for human error, in recognition that this is a common theme in security incidents occurring, the Council is exploring whether measures could be put in place to reduce the likelihood of such incidents occurring. In addition, the Information Governance Team has introduced a revised information security incident procedure, which includes a matrix for assessing the level of risk an information security incident poses, as well as sets out a process for implementing recommendations following investigations.

There have been no data breaches during this period that met the threshold to be reported to the ICO.

In addition to the above, the Council has also taken the following measures to reduce the likelihood of information security incidents occurring:

- A file storage review, including digitisation and destruction of hard copy files;
- An Information Governance Review, which involved a comprehensive assessment of the Council's information management policies and procedures to form an Information Governance Framework;
- Advice has been given to relevant services on specific areas of compliance; and
- A new process for reporting information security incidents has been implemented which requires officers to complete a form detailing the incident and to telephone the Information Governance team to enable them to assess whether any urgent actions need to be taken.

5. Organisational Compliance with Regulatory Requirements

Changes to legislation during 2023/2024

There have been no significant changes to primary legislation in the reporting period. The EU GDPR is an EU Regulation which no longer applies to the UK. Following the transition period, EU law was automatically transferred into UK law. The UK's version of GDPR is essentially a copy of the EU's GDPR with some subtle differences.
The Information Governance Team continues to monitor and share where necessary, guidance and developments from the ICO.

There is a new Data Protection and Digital Information Bill that is currently passing through the House of Lords. The Information Governance Team is keeping this under review and will seek to implement any necessary changes should the bill be passed.

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 2023 – 31 March 2024 there was no need for any data protection assessments to be carried out.

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 90%.

Currently, the timing of the completion of the training depends on when each staff member last completed it. During the period 1 April 2023 to 31 March 2024, 81% of staff completed the training. Although this figure is below target, it does not account for any staff members who may be on extended leave e.g. sickness, maternity leave, etc., however, the completion of training will be kept under review to ensure that staff continue to stay up-to-date and complete it when they are required to do so.

The training programme will also be reviewed this upcoming year to ensure it is fit for purpose and covers all the required areas that staff need to be trained on. As part of that review, the training will be updated annually, with all staff expected to complete it at the same time each year (April), to ensure going forward that completion rates can be properly monitored and if there are staff that have not completed it, then this can be addressed, as appropriate.

In addition to the mandatory annual training, training on data protection and information requests 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.

Training has also been provided to Members through member spotlight sessions that were held in May 2023.

In the upcoming year, it is intended that as well as the annual mandatory training there will be more focussed sessions as part of the Corporate Governance Programme and service-focussed sessions, where required.

Policies

The Council’s information governance policies have been reviewed as part of the Information Governance Review. These policies have been updated where necessary and will form part of a new Information Governance framework.

The Information Management Policy was last considered by Cabinet in September 2023 and the new policies will follow the usual process for review as part of the suite of Corporate Governance Policies this year.

In addition to reviewing the policies, the Information Governance Team has also been working on an information governance toolkit to support officers in understanding their obligations. The toolkit includes policies, guidance and flowcharts. The team has also reviewed all of its templates to ensure they are up-to-date and clear.

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 IASM (Information Assurance for Small and Medium Enterprises) organisation. Any critical, medium, and high risks are resolved The IT security health check is an assessment of our security posture, where the internal and external network is check for vulnerabilities, to ensure that we are following best practice, systems and applications have been patched and updated as well as overall security health of our IT landscape

- 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 PSN (Public Sector Network) accreditation for 2024/25. The Public Sector Network (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 we are looking at other ways to improve the uptake of this training. A yearly mandatory cyber security training is also undertaken and this completion rate for this in 2023 was 91.78%

- 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.

- Improved business recovery arrangements have been implemented to minimise recovery time. Accreditation to Cyber Essentials and the Public Services Network has been secured.

- The latest audit / assessments all confirm a secure environment with reasonable assurance. Some formalisations of processes are required and review of the backups restoration window. 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 27 medium and 102 Low Vulnerabilities, which the Council is working to mitigate using the tool that has been purchased.

- An annual external audit of IT assessed the organisation's IT arrangements in a range of areas against best practice. The outcome of the audit in 2023 was, reasonable assurance, with three high recommendations and four medium, which were mainly around backup and formalisation of processes. Plans have been put in place to address these and provide assurance that the Council's IT arrangements are solid, sound and secure. All remediations from the 2023 IT audit have been completed.

- 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. We now have 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.