Appendix 1

SENIOR INFORMATION RISK OWNER REPORT 2025-26

1. Introduction

The responsibility for effective information risk management is shared by all staff across the Council.

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 include:

- 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
- 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
- Keep the Council's information governance framework under review, taking account of any changes required because of new or amended legislation, guidance, or other relevant factors
- Review key information governance risks and monitor through the Councils Corporate Risk Register and escalate where appropriate to Corporate Leadership Team and Members.

2. Purpose of the Report

The purpose of this report is to provide an overview of the Council's compliance with regulatory requirements and to outline how information risk has been managed across the organisation over the past year. It demonstrates how the Council has continued to meet its statutory obligations in relation to the processing of personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as well as its duty to act transparently through compliance with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

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
- 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 EIR applies to all information which relates to the environment, 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. 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 to its Audit and Governance Committee quarterly on how it is performing in relation to responding to information requests.

The following table sets out the number of requests received and responded to within the period 1 April 2025 - 31 March 2026:

Request Type	Number of Requests
FOI	641
EIR	62
SAR	90

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

Request Type	Number of Requests
FOI	655
EIR	17
SAR	54

From the above figures it can be noted that:

- There has been a slight decrease in the number of FOI requests received.
- There has been a significant increase in the number of EIR requests received.
- There has been a significant increase in the number of SAR requests received.

There are several factors believed to have contributed to the increase in the number of Subject Access Requests (SARs) received, including:

• Increased public awareness of data protection rights, particularly the right of access under data protection legislation.

• Greater use of SARs in complaints, disputes, and legal proceedings, where individuals seek access to their personal data to support their position or challenge decision-making.

There are several factors believed to have contributed to the increase in the number of Environmental Information Regulations (EIR) received, including:

• Training and awareness – The definition of environmental information under the Environmental Information Regulations (EIR) is broad and includes information such as policies, plans, and strategies. As awareness and understanding of the scope of the EIR has improved, requests that may previously have been handled under the Freedom of Information Act are now appropriately treated as EIR requests.

• Planning and development activity – Increased interest in local planning and development activity, which may include residents, community groups or other stakeholders, has resulted in a higher volume of requests for environmental information relating to these matters.

The statutory timescale for responding to Freedom of Information and Environmental Information Regulations requests is 20 working days, which may be extended by a further 20 working days where a request is complex or voluminous. The statutory timescale for responding to Subject Access Requests is one calendar month.

The table below sets out the percentage of requests responded to within the statutory timescales:

2025-26	Q1	Q2	Q3	Q4
FOI (Total Received)	161	154	161	165
FOI (% responded to within the statutory timeframe)	91%	90%	93%	95%
EIR (Total Received)	10	15	14	23
EIR (% responded to within the statutory timeframe)	90%	87%	93%	96%
SAR (Total Received)	25	24	19	22
SAR (% responded to within the statutory timeframe)	100%	87%	95%	90%

Overall, the table above shows that the Council's target response rate of 90% has largely been achieved throughout the year.

An internal review is a formal process that allows a requestor to ask the Council to reconsider how their request was handled where they have expressed dissatisfaction with the outcome.

The below table shows the number of internal review requests per quarter. This covers FOI, EIR & SAR requests.

Q1	Q2	Q3	Q4
4	3	2	6

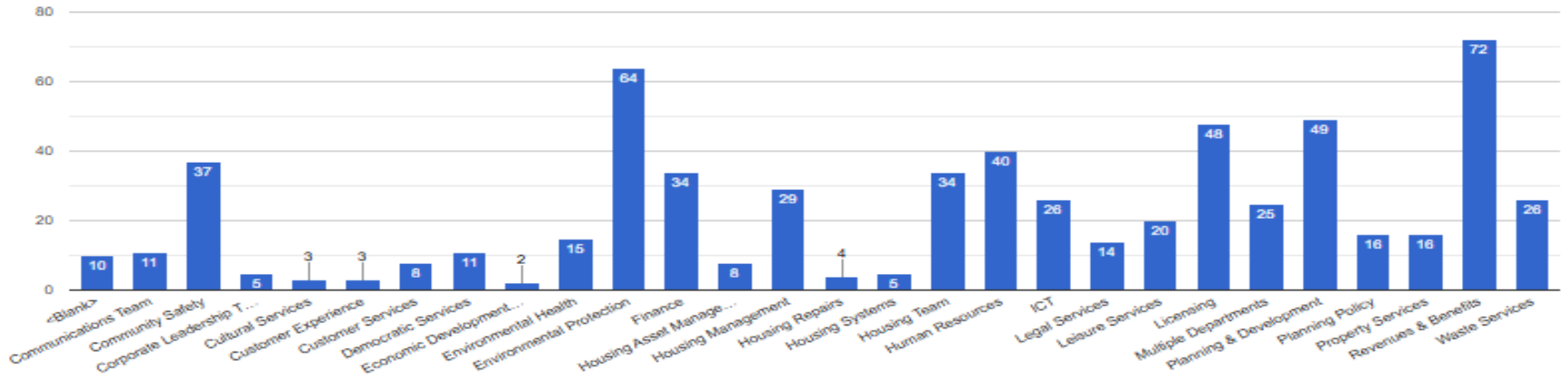
The above table shows a total of 15 internal reviews were requested during the period 01 April 2025- 31 March 2026. The request for internal reviews has seen a significant increase on the 4 internal reviews that were requested during the period 01 April 2024- 31 March 2025.

The Information Governance Team believes that the increase in internal review requests is due to greater awareness among requesters of their right to seek a review before escalating a matter to the Information Commissioner's Office (ICO). This awareness has increased because of clearer ICO guidance and improved signposting.

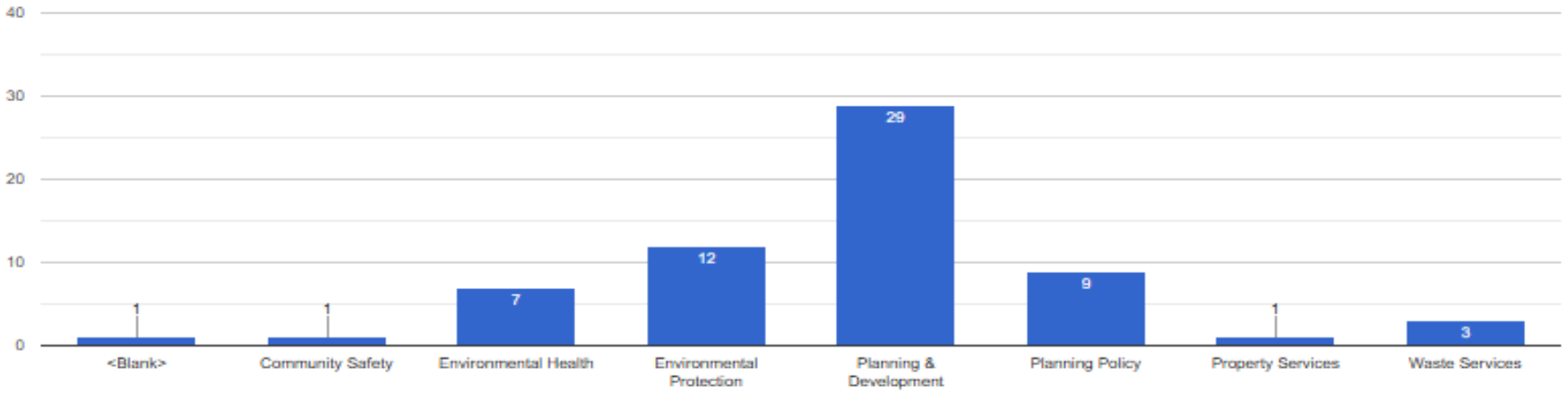
It is also recognised that requests are becoming increasingly complex and voluminous, which can result in partial disclosures, extensions or refusals. These outcomes are more likely to lead requesters to seek an internal review.

In addition, internal review requests are often linked to wider issues such as complaints, planning or development matters, environmental or community concerns or service delivery disputes. In such cases, requesters may use the internal review process as part of a broader challenge to the Council’s actions or decisions.

The following table represents the number of FOI requests received by service area:



The following table represents the number of EIR requests received by service area:



The above tables show that Revenues and Benefits and Environmental Protection received the highest number of FOI requests. Planning and Development received the highest number of EIR request.

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 37 information security incidents reported during the period of 1 April 2025 – 31 March 2026. Each security incident has been investigated by a member of the Information Governance Team and where appropriate, measures and mitigations have been made to prevent the reoccurrence of similar incidents.

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

Of the 37 information security incidents reported, these were categorised as follows:

29 Confidentially Breaches
8 No breach

The table below provides a breakdown of the reported information security incidents by incident category:

Verbal disclosure of personal data	2
Data emailed to incorrect recipient	11
Failure to redact	4
Data posted to incorrect recipient	4
Breach of consent or data minimisation principles	4
Loss/theft of device containing personal data	2
Unauthorised Access	1
Data used beyond its intended purpose	1

The highest incident category related to data being emailed to an incorrect recipient. This is reflective of the high volume of email communications across the organisation and mirrors the most common category of breaches reported to the Information

Commissioner's Office. To address this risk, the Information Governance Team is working in collaboration with the IT Team to implement tools available within the Microsoft Purview suite, which will strengthen data governance controls and help reduce the likelihood of incidents associated with this type of breach.

During the reporting period, three data breaches met the threshold for notification to the Information Commissioner's Office. Each incident was investigated in line with the Council's Data Breach and Information Security Procedure and assessed against the corporate risk matrix. It was determined that the potential risk to the rights and freedoms of the affected individuals met the statutory threshold for notification to the ICO in accordance with Article 33 of the UK GDPR.

Immediate mitigation actions were implemented to reduce any ongoing risk to the individuals concerned. In addition, further recommendations were provided to the relevant service areas to minimise the risk of similar incidents occurring in the future.

The Information Commissioner's Office has responded in respect of two of the reported incidents and has confirmed that these cases have now been closed. No further communication has been received from the Information Commissioners Office in relation to the third breach.

While it is recognised there will be a degree of human error, the Council has implemented the following measures to reduce the likelihood of information security incidents occurring:

- Launch of an updated mandatory online information governance and data protection training course on 1 April 2025.
- Ongoing Data Protection training delivered through Corporate Governance training sessions, supporting continued staff awareness and compliance.
- Completion of site audits at Whitwick Business Centre, Customer Services Centre, and the Depot to provide assurance of compliance with data protection requirements.
- Regular review and updating of policies and procedures, supported by the development and implementation of guidance documents for staff.
- Exploration and utilisation of Microsoft Office functionality to reduce information security risks, including the use of tools such as email classifications and data handling controls.
- Review and update of core data protection documentation, including the Information Asset Register (IAR) and Records of Processing Activity (ROPA), to strengthen compliance and accountability.
- Ongoing review of Data Sharing Agreements, Data Processing Agreements, and Data Protection Impact Assessments (DPIAs) to ensure they remain current, lawful, and proportionate.

4. Organisational Compliance with Regulatory Requirements

Data (Use and Access) Act 2025

The Data Use and Access Act 2025 (DUAA) received Royal Assent on 19 June 2025. The Act amends and clarifies aspects of the existing data protection framework but does not replace the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), or the Privacy and Electronic Communications Regulations (PECR).
The Act is being implemented on a phased basis between June 2025 and June 2026, supported by secondary legislation. The Information Governance Team is monitoring these developments and will implement appropriate actions and training to ensure continued compliance.

The Information Governance Team is also working to formalise the Council's processes to support the new statutory right for data subjects to complain under the Act. While data protection complaints were already handled by the Information Governance Team, the introduction of this right has prompted a review to ensure the process is clear, easily accessible to data subjects and supported by updated policies and procedures.

Data Protection Impact Assessments

The Council manages a wide range of personal information that is essential to the delivery of its services. The Council has a statutory responsibility to ensure that its information systems and supporting processes meet requirements relating to security, confidentiality, data protection and data quality.

When new policies, systems or changes to existing practices involving the processing of personal data are introduced, the Council undertakes Data Protection Impact Assessments (DPIAs). DPIAs help to identify and mitigate risks to individuals' privacy and ensure that appropriate measures are in place to protect personal data throughout the lifecycle of a project or service.

During the period 1 April 2025 to 31 March 2026, a total of 17 DPIAs were completed, compared to 10 in the previous reporting year. This increase reflects the continued delivery of mandatory e-learning and Corporate Governance training, alongside improved staff awareness of the requirement to complete an initial DPIA screening where a project or service involves the processing of personal data. The requirement to consider whether a DPIA is necessary has been implemented within the Council's procurement processes to ensure that any new projects or services being procured are appropriately assessed for data protection risks at an early stage.

All completed screenings are reviewed by the Information Governance Team to determine whether a full DPIA is required. While a DPIA is mandatory where processing is assessed as high risk to the rights and freedoms of individuals, it is also used as a valuable early stage tool to identify and manage data protection risks in new or changing projects and services.

In collaboration with the Council's Project Officer, an internal online Data Protection Impact Assessment form has been developed for use via the staff portal. This will support officers in completing DPIAs more effectively, provide a clear audit trail of updates and amendments and improve oversight and management of DPIA reviews. The form has been built and demonstrated within the Information Governance Team, with the next stage being roll out to wider teams for user testing.

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.

The training programme scheduled for completion during the year was reviewed and updated to ensure it remained fit for purpose. In addition, further targeted training is planned to focus on Freedom of Information (FOI), Environmental Information Regulations (EIR), and Data Protection requests.

Audit

The Data Protection audit was completed during 2025/26, achieving a 'reasonable' level of assurance. Two medium recommendations were made, both of which have now been completed and closed.

Artificial Intelligence (A.I)

The Council undertook a trial of Microsoft Copilot involving selected users from a range of service areas. Prior to the commencement of the trial, users were provided with guidance and training to support data protection requirements. The trial has now concluded and the Information Governance Team will work closely with the Transformation Team to ensure that data protection compliance is maintained in respect of any future roll out. Consideration is also being given to what supporting documentation, including policies and procedures, may be required to underpin the appropriate use of AI technologies. The associated DPIA will remain under regular review and be updated as necessary.

Policies and Procedures

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 February 2026, following presentation to the Audit and Governance Committee on the 4 February 2026. The policies included in the framework include:

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

The following procedure documents form part of the Information Governance Toolkit:

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

The Surveillance Camera Technologies Procedure is currently in draft form and once finalised, will form part of the Council's governance toolkit. The procedure sets out the lawful, proportionate and transparent use of the Council's surveillance technologies. A cross service working group has been established to progress the development of the procedure and to ensure that data protection compliance is embedded on a Council wide basis. The procedure will be supported by service specific guidance documents.

The policies and procedures are 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 25/26, the Council had no critical, five high and six medium issues. The high and medium issues have now been remediated. The Council is currently working on renewing its Public Sector Network (PSN) accreditation for 25/26. The

PSN accreditation, provides assurance to the Cabinet Office that the Council has maintained compliance for connecting to government networks

• Phishing campaigns are conducted quarterly 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. Completion rates remain below the desired level, which presents a compliance risk. Further measures are being explored to improve uptake and ensure mandatory training requirements are consistently met. Annual mandatory cyber security training is also undertaken and this completion rate for this in 2025 was 89%

• 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 are in progress

• All 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 34 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 an update on the IT Health Check, which was well taken

• 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

5. Priorities for 2026/27

The Council's information governance priorities for the forthcoming year are as follows:

- Data Use and Access Act Implementation

To continue monitoring, interpreting and implementing requirements arising from the Data Use and Access Act and any associated secondary legislation. This includes incorporating the newly introduced data subject right to complain into the Council's existing corporate complaints framework. The updated online complaints process is scheduled to go live by 19 June 2026.

- Strengthening DPIA Compliance

To enhance Data Protection Impact Assessment (DPIA) compliance through the rollout of a standardised online DPIA form. This will support improved consistency, oversight, and audit capability across service areas, ensuring that privacy risks are identified and mitigated effectively.

- Surveillance Camera Governance

To implement the Council's Surveillance Camera Technologies Procedure and supporting documentation to strengthen compliance with legislative and regulatory requirements. This will include a comprehensive review of existing surveillance technologies currently deployed across the Council to ensure continued compliance and appropriate governance controls.

- Microsoft Purview Implementation

To further embed Microsoft Purview controls to enhance the security, classification, and management of the Council's information assets, supporting improved data protection and information security outcomes.

- Review of Statutory and Corporate Information Governance Documentation

To continue a review and update of key statutory and corporate information governance documents, including Privacy Notices, Record of Processing Activities (ROPA), Information Asset Register (IAR), Retention Schedules, Policies and Procedures.

6. Overall Assurance

Based on the work undertaken during 2025/26, the SIRO can provide reasonable assurance that the Council has appropriate information governance arrangements in place and is broadly compliant with its statutory obligations.

While the overall framework is effective, areas for continued focus include:

- Reducing incidents caused by human error
- Embedding new governance arrangements
- Managing increasing volumes and complexity of requests