COTSWOLD
District Council

Information Governance &

Senior Information Risk Officer (SIRO) Report 2024/25

1 Executive Summary

Over the past year, progress has been made to reduce the turnaround time on Subject Access Requests, Freedom of Information requests, reducing information risk for the Council and growing the maturity of the approach to data and information.

Progress has also been made in improving the approach to information governance, information risk and cyber security across the Council and while there are challenges that remain to be resolved, there are clearly defined actions for the future.

This first report provides a detailed look at the Council's key actions regarding information governance and information risk management.

The report provides both a backward-looking view of the actions, plans, opportunities and challenges related to information risk and governance during 2024/25 and satisfies the requirement for the Senior Information Risk Owner (SIRO) to provide an annual report and a forward-looking view of planned activities for the next year.

2 Background

2.1 Regulatory, Strategy & Policy Framework

The UK GDPR and Data Protection Act 2018 (DPA 2018) are the primary pieces of legislation regulating data protection in the UK.

The proposed Data Protection and Digital Information Bill (DPDI Bill) did not pass through Parliament before the General Election; instead the Data (Use and Access) Bill received Royal Assent in June 2025. The Data (Use and Access) (DUA) Act 2025 complements, rather than replaces, existing legislation like the UK GDPR and the Data Protection Act 2018. The Act aims to make it easier and more secure for data to be shared and used, such as through new Smart Data schemes and digital verification services.

Key actions from the DUA Act 2025:

Key Changes	**Plans**	**Responsible Officer**
Subject Access Requests (SARs) – The Council must now only conduct "reasonable and proportionate" searches. The time limit for responding can also be paused if the Council needs more information from the requester.	We have updated our internal SAR procedures and we are now compliant with the DUA Act.	Compliance Manager
Cookies: Exemptions have been created for certain cookies, such as those used for statistical purposes, to be used without user consent.	The Council Cookies Privacy Notice has been updated with DUA requirement. This action has been completed.	DPO
Automated decision-making: Restrictions on automated decision-making have been relaxed, allowing for broader use of these systems, though safeguards are still required.	Automated decision-making review undertaken on Council processing activities completed. Privacy Notices have been updated.	DPO
Internal complaints procedure: Council is now required to have an internal complaints procedure for data protection issues. Individuals must complain to the organization first before escalating to the Information Commissioner.	We have updated our internal complaint process and aligned all data protection complaints received with our generic complaints process. we are compliant with the DUA Act.	Compliance Manager

The Information Commissioner's Office (ICO) has undergone several internal structure changes, most recently with the introduction of the DUA Act 2025. The new structure is called the Information Commission (IC).

IC has announced a set of commitments to support the government's growth agenda. These include introducing a statutory code of practice for businesses developing or deploying Artificial Intelligence (AI); simplification of the Privacy and Electronic Communications Regulations (PECR) consent requirements (which mainly relate to cookies and other tracking technology) and publishing new guidance on international data transfers.

The above matters continue to be monitored by the ICT Audit & Compliance Manager (Data Protection Officer (DPO)), who will update the Corporate Leadership Team as required.

Privacy & Electronic Communications Regulations (PECR) consent requirements:

Key Actions Required	Plans	Responsible Officer
General rule: The Council will need prior consent to send unsolicited direct marketing to individuals.	Consent Review Marketing activities completed July 25. Council Communication service 'Communicating with our residents' website pages and Privacy Notice updated with PECR consent requirements Sept 25	DPO
Existing customers: The Council can email existing customers with marketing for similar services without consent, provided they had the chance to opt out when their details were collected and are given an easy way to opt out of future marketing	The Council's Communications services marketing procedures are now compliant with PECR consent requirements. Review completed by DPO in Aug 25.	DPO
Obtaining consent: The Council required to have reliable method is to provide opt-in boxes where individuals can clearly indicate they want to receive marketing. **Opt-out:** All marketing communications must include a simple way for recipients to unsubscribe.	The Councils Communications services Consent marketing procedures is now compliant with PECR consent requirements. Review completed by DPO in Aug/Sept 25.	DPO

The Council's vision for managing information, the principles supporting that vision and the context and challenges faced by the Council are detailed in the relevant policies and guidance documents:

Policy	Review	Responsible Officer
Data Breach Policy & Procedures – Compliance with UK GDPR Article 33 & 34	Completed June 2025	Compliance Team
Council & Publica Privacy Notices - Compliance with UK GDPR Article 5 (Data Protection Principles) & DUA Act 2025 update	2026: On-going review of 60 Privacy Notices	Compliance Team
Data Protection Policy – Compliance with UK GDPR Article 5 (Data Protection Principles) & DUA Act 2025 update	February 2026	DPO

Information & Data Retention Schedule - ensures compliance with Article 5(1)(e) of the UK GDPR by establishing and enforcing rules for how long personal data is kept, ensuring it is not stored longer than necessary for the original purpose	March 2026	Compliance Team
ICT Acceptable Use Policies – ensures compliance with UK GDPR Article 5, Article 32 Security of processing, Computer Misuse Act 1990 (UK), Malicious Communications Act 1988	March 2026	ICT Audit & Compliance Manager/DPO
Record of Processing Activities – which is a detailed written log of all personal data processing, ensures Compliance with Article 30 of the UK GDPR	July 26	Compliance Team

2.2 Roles & Responsibilities

Before November 2024, the role of SIRO was under the remit of Publica. Since then, the Chief Executive has taken over this role and responsibilities including:

- working closely with the DPO.
- overseeing the strategic management of information-related risks.
- ensuring alignment with business objectives.
- promoting a culture that protects information.
- owning information risk management policies and processes; ensuring they are implemented.
- advising on information risk management processes and assurances.
- owning the ICO incident management framework.
- producing an annual report on information risk and governance, covering progress and plans, of which this is the first.

The SIRO’s overall role is supported by the Director of Governance & Development and the internal Governance Group.

The Data Protection Officer (DPO) is a statutory role required by Article 37 of the UK GDPR and Section 69 of the Data Protection Act 2018 to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner.

3 Looking Backwards

3.1 Data Breaches

	2024/25			
	Q1	Q2	Q3	Q4
Total Breaches	-	3	1	1
Low Level	-	3	1	1
Medium Level	-	-	-	-
High Level	-	-	-	-

3.2 Subject Access Requests

	2024/25			
	Q1	Q2	Q3	Q4
Requests Received	6	3	-	4
Requests Completed & Issued	3	2	-	4
Requests Open/On Hold*	3	1	-	-

3.3 Access Controls

Access controls are the mechanisms and policies that determine who or what is permitted to access specific resources such as data, applications and physical locations. It is a security measure that verifies the user's identity (authentication) and then grants or denies access based on predefined rules and permissions (authorisation). Starters, leavers and transfers are crucial security processes which ensure starters are onboarded with the correct access, existing staff who move jobs have the correct access and those who leave the organisation have their access revoked.

3.4 Data Retention

Effective management of Council records is essential to support service delivery, meet legal requirements and manage information-related risks. Following a SWAP Audit, a Council-wide review of our current Retention Schedule is being undertaken in 2025/26. The review will ensure schedules are aligned to legal and operational requirements and reflect all activities where data is held in compliance with the Council's Document Retention and Disposal Policy.

The Council also maintains its Information Asset Register, providing a key governance mechanism for overseeing information assets and associated risks.

3.5 Data Destruction

Departments continued to carry out routine destruction of information assets in line with approved retention schedules, using established procedures to ensure the secure disposal of both digital and physical records. A review of the organisation's retention schedule is under way and scheduled for completion in the first quarter of 2026; this work includes a review of departmental record destruction procedures which will strengthen overall assurance around disposal practices.

3.6 Freedom of Information/Environmental Information Requests

Under the Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR), individuals are entitled to ask the Council for a copy of information it holds.

	2024/25			
	Q1	Q2	Q3	Q4
Requests Received	106	100	120	117
Answered within 20 days	93 87.7%	95 95%	107 89.2%	96 82.1%
Answered after 20 days	13 12.3%	5 5%	13 10.8%	21 17.9%

3.7 Training & Awareness

Communications related to data security, cyber security and phishing are a regular communication topic for all officers and elected members. Over the past year there has been communication related to these topics which is raising awareness and both data protection and cyber training is a mandatory part of each new staff's induction programme with annual refreshers for existing staff.

Completion rates for the annual training programme have a target of 95% for Cyber Security & Data Confident (GDPR) training, actual achieved is 93%. The Information Commission does not set a specific "target rate" for GDPR training completion but expects training to be ongoing and effective.

Messages through a variety of communication channels are provided to staff alerting them to the need to protect personal data, be vigilant around cyber security and to use data appropriately.

3.8 Data Sharing Requests

The Council continues to work closely with partner organisations and shares data where appropriate to support service delivery. Requests for the disclosure of information about identifiable individuals, including those made under Schedule 2 or to confirm a person's status, were assessed on a case-by-case basis to ensure a clear legal basis for sharing and full compliance with data-protection requirements. Data Sharing Agreements were developed and updated for both short and long-term initiatives across a range of departments, with appropriate safeguards and privacy notices in place to ensure the public remains informed about how their information is used.

3.9 Data Policies & Guidance Documents

Policy	**Review**	**Responsible Officer**
Data Protection Policy – Compliance with UK GDPR Article 5 (Data Protection Principles) & DUA Act 2025 update	Dec 2025	DPO

Data Breach Policy & Procedures – Compliance with UK GDPR Article 33 & 34	Jun 2025	Compliance Team
Information & Data Retention Schedule - ensures compliance with Article 5(1)(e) of the UK GDPR by establishing and enforcing rules for how long personal data is kept, ensuring it is not stored longer than necessary for the original purpose	Nov 2025	Compliance Team
ICT Acceptable Use Policies – ensures compliance with UK GDPR Article 5, Article 32 Security of processing, Computer Misuse Act 1990 (UK), Malicious Communications Act 1988	Mar 2026	ICT Audit & Compliance Manager | DPO
Council & Publica Privacy Notices - Compliance with UK GDPR Article 5 (Data Protection Principles) & DUA Act 2025 update	Jan 26 – Dec 26: On-going review of 60 Privacy Notices	Compliance Team
Record of Processing Activities – ensures Compliance with Article 30 of the UK GDPR	Jul 26	Compliance Team

3.10 Cyber Security

Cyber Security is reported via the Council Audit and Governance Committee annually. Additional briefings for councillors and senior officers are available on request.

The Council operates a dedicated Cyber Security Team as part of its shared service arrangements with other Councils. This allows the Team to attract and retain staff with industry recognised Cyber Security qualifications. Investment by the Council has ensured the security solutions deployed are suitable for the task and configured correctly.

The Council obtained its Annual Public Sector Network (PSN) Code of Compliance certification in June 2024 and again in June 2025. This process includes security assessment by third party experts both internally and externally. The results of these assessments are reviewed by the Cabinet Officer.

The Council achieved the MHCLG Cyber Assessment Framework (CAF) Ready status in 2024. As a result of the preventative measures taken, there were no cyber security incidents that had a negative impact upon the Council in 2024/25.

4 Looking Forward

4.1 Strategic Direction - Future Programme of Work and Key Focus Areas

The strategic direction for information risk is to reduce information risk across the Council and associated organisations by ensuring that the right practices are in place and accountabilities understood.

Key areas of focus are:

- Risk Register
- Internal Audit
- External Audit
- Data Retention and Destruction
- Other regulator observations
- LGR and data sharing
- ICT environment (emphasis on shared platforms and data security)
- AI
- Microsoft 365 Implementation and Windows 11 Rollout

4.2 Staff Awareness

People are the first line of defence and the weakest link. Ongoing education and awareness of the importance of maintaining vigilance around cyber will continue. The approach to updates via regular communication to remind officers and members of the need for vigilance will continue,

4.3 Risk Register

The Council's strategic risk register is maintained by responsible officers which is regularly reviewed by the Corporate Leadership Team. The register includes a 'Compliance – GDPR/Data Breach' section which mitigates the risk of the Council not having adequate internal controls around the management of its data resulting in a data breach.

5 Concluding Comments

The Council operates in a challenging environment with growing cyber threats, constantly changing digital world and increasing pressure to do more with less. Embracing the use of digital tools and data is critical, along with ensuring that officers can be the vital first line of defence. Maturing the way in which data and information are managed and supporting this with effective processes and policies are some of the tools in the arsenal. T eams continue to make progress in enhancing the measures taken to mitigate information risk, uplift understanding of officers and to ensure that robust cyber security measures are in place.

The collaborative efforts across various teams have resulted in strengthened controls, improved training and a more resilient infrastructure. Constant improvements and ensuring the momentum is maintained will allow the Council to keep improving the stance towards information risk and ensure that we keep our resident data safe and secure.