Information Governance Strategy 2025 – 2028

Version History

File reference	Date	Author/amend	Description	Status
Information Governance Strategy	5th February 2025		Feedback changes	Draft
	21st March 2025		Approved by SIGG	Final
	9th April 2025		Approved by CMT	Final

Summary

The Information Governance Strategy sets out the strategic direction for enhancing our Information Governance capabilities and embedding a strong Information Governance culture across Midlothian Council.

1.0 Background

1.1 This Information Governance Strategy has been developed in response to the legislative requirements in relation to the management of information. It is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information.

1.2 While this document focuses on Information Governance, it also relates to Information Management. Although these terms are often used interchangeably, Information Governance specifically ensures compliance with rules and regulatory requirements. It also defines roles, responsibilities, and the key functions involved in managing information effectively.

1.3 In recent years, new legislation has introduced additional responsibilities for local authorities. To ensure compliance and effectively manage its valuable information assets, the Council must adopt a strategic, organisation-wide approach to Information Governance. This strategy provides a clear framework and direction, enabling the Council to enhance its services by improving the management, accessibility, and use of information across all areas.

1.4 The rapid growth of digital services, the progression of cloud technology, emerging cyber threats, and the expanding role of Artificial Intelligence (AI) require a flexible and responsive Information Governance strategy. While advancements in data processing technology create opportunities for innovation and service improvements, they also bring challenges related to data privacy, ethical considerations, and regulatory compliance.

1.5 To tackle these challenges, the Council must actively monitor and adapt to changes in legislation, industry best practices, and cybersecurity threats. By taking a forward-thinking approach to Information Governance, Midlothian Council can leverage new technologies while ensuring regulatory compliance and maintaining public trust.

1.6 To ensure strong oversight, the Strategic Information Governance Group (SIGG) oversees the implementation of best practices across Midlothian Council. Led by the Senior Information Risk Owner (SIRO), the group provides strategic direction and support to maintain effective Information Governance.

1.7 The SIGG supports wider corporate governance requirements to manage information appropriately by providing strategic leadership, guidance and support to Council Services. The SIGG is not responsible for implementing the compliance requirements, as that is the responsibility of the individual Council services.

2.0 Our Vision and what success will look like

2.1 Our goal is to create an environment where information is efficiently managed, protected from risks, and available for decision-making and service delivery. This will support Midlothian Council's commitment to transparency, accountability, and innovation.

2.2 To achieve our vision, the following principles will be embedded across the Council:

- **Compliance with all legislative and regulatory requirements:** Ensuring adherence to the Data Protection Act, Public Records (Scotland) Act, Freedom of Information Scotland Act and other relevant laws is fundamental to our governance framework. Compliance is not just a legal obligation but a means of ensuring trust and accountability.
- **Secure storage and controlled access:** Protecting information based on a 'need-to-know' basis minimises risks and enhances data security. Strict access controls will be maintained to prevent unauthorised use.
- **Availability of accurate information:** Ensuring data is accessible when required while maintaining accuracy supports effective decision-making and service delivery.
- **Appropriate information sharing:** Enabling controlled and appropriate data-sharing practices within and outside the Council ensures that information is used responsibly, balancing transparency with confidentiality.
- **Training and capacity-building:** Providing staff with the knowledge to uphold Information Governance responsibilities is crucial to sustaining a strong governance culture. Regular training and awareness initiatives will reinforce staff responsibilities and best practices.
- **Ethical AI and data management:** Ensuring AI use aligns with regulatory requirements and ethical standards is essential as automation and data analytics become more embedded in Council operations. Clear frameworks will guide AI implementation to ensure responsible innovation.

3.0 Current position: The drivers of our strategy

3.1 Legislative and Regulatory Drivers

Midlothian Council operates within a strict legal and regulatory environment. Compliance with UK GDPR, the Public Records (Scotland) Act, and other data protection laws is critical to our strategy. Additionally, evolving AI and data ethics regulations must be addressed to mitigate risks associated with emerging technologies.

As new legislation is introduced, our governance framework will be continuously reviewed and adapted to maintain compliance. The introduction of AI regulations, greater scrutiny on cybersecurity practices, and evolving data protection standards mean that the Council must stay ahead of regulatory changes to ensure ongoing compliance and operational resilience.

3.2 Strategic Drivers

Aligning IG strategy with broader Council objectives ensures a modern and efficient approach to data management. Key strategic drivers include:

- **Holistic Working:** Breaking down silos to facilitate seamless data access and use. Improved collaboration ensures that information flows efficiently across departments, improving service delivery.
- **Modernisation:** Adopting digital solutions to enhance data management capabilities. Leveraging technology enables greater efficiency and reduces reliance on outdated processes.
- **Security & Compliance:** Strengthening cybersecurity measures and ensuring regulatory adherence is essential for safeguarding Council data and maintaining public confidence.
- **Continuous Improvement:** Regular updates to processes and policies based on evolving risks and best practices ensure that the Council remains proactive in its approach to information governance.

4.0 Who will deliver?

4.1 The Strategic Information Governance Group (SIGG) will use this strategy and implement it through the annual SIGG action plan. The implementation of the strategy is dependent on the support of senior management ensuring that adequate time and resources are allocated to the task. This includes ensuring that Directorate SIGG members are able to fulfil their commitments when supporting their services to complete the SIGG action plan.

4.2 The work of the SIGG will be overseen by the Council's Senior Information Risk Owner (SIRO) who will report progress and issues to the Corporate Management Team.

4.3 Each Council Directorate should have a dedicated resource responsible for Information Management implementation with support from the SIGG.

4.4 Each business area must identify an Information Asset Owner (IAO) to take ownership of its information assets. These individuals will be responsible for the confidentiality, integrity and availability of that asset.

4.5 The work of the SIGG will be supported by the information management specialists that include:

- **Senior Information Risk Owner (SIRO) (Chair).** Provides overall leadership and direction.
- **Cyber Security and Information Governance Manager.** Ensures technical security measures are in place.
- **Data Protection Officer.** Oversees compliance with data protection laws.
- **Information Compliance Officer.** Manages regulatory and legal compliance aspects.
- **Democratic and Document Services Records Team Lead.** Oversees document and records management.
- **Principal Solicitor.** Provides legal guidance on information governance matters.
- **Principal Data and Information Governance Officer.** Ensures data management practices align with strategic objectives.
- **Internal Audit Representative.** Ensures robust governance and internal compliance.
- **Compliance Manager.** Supports data protection and Records Management compliance
- **Directorate Representatives.** Provide insights and oversight within their respective service areas:
    - **Place: Lead Performance and Improvement Officer.**
    - **Children, Young People, and Partnerships (CYPP): Learning Estate Resource Officer.**
    - **Health and Social Care (HSC): Performance Programme Manager (NHS).**

5.0 What we will do

5.1 To successfully implement information governance, we must focus on key areas that ensure compliance, security, and efficiency in data handling. These focus areas provide a structured approach to managing risks and opportunities related to information governance.

Each area has specific objectives aimed at improving our data governance framework, ensuring that data protection remains a priority while enabling digital transformation and efficiency. Our focus areas include:

- **Information Governance Framework:** To ensure effective implementation of information governance, we will establish comprehensive policies and procedures that promote compliance and provide a structured approach to managing information risks. These frameworks will guide the management and protection of data across the organisation**.**

- **Training & Awareness:** A cornerstone of successful information governance is equipping staff with the necessary knowledge. We will deliver targeted Information Governance training programmes to ensure that all employees understand their roles and responsibilities and are equipped to handle information in accordance with governance standards.

- **Records & Data Management:** We will prioritise the proper management of records and data by adhering to statutory requirements and best practices. This includes ensuring that all records are systematically stored, classified, tracked, and disposed of according to legal and regulatory standards, mitigating the risk of non-compliance.

- **Security for Personal Data:** Protecting personal data is critical. We will implement robust security measures designed to prevent data breaches and unauthorised access, ensuring that all personal information is handled with the highest level of security and confidentiality.

- **Data Sharing:** As we navigate digital transformation, responsible data sharing will be prioritised. We will ensure that all data handling practices comply with relevant laws and regulations, particularly around data privacy, to protect both individuals and the organisation.

- **AI Compliance:** Ethical use of AI will be a key focus. We will ensure that our use of AI aligns with legal and ethical standards, maintaining transparency, accountability, and fairness in decision-making.

- **Risk Management:** Proactively identifying and mitigating risks related to information governance is essential to safeguarding the organisation. We will implement a risk management approach that allows us to identify potential threats, address them swiftly, and continuously monitor the effectiveness of our governance measures.

6.0 How we will do it

6.1 The Strategic Information Governance Group (SIGG) will meet every quarter to monitor progress, identify risks and amend the action plan.

6.2 We will implement this strategy through a structured approach that ensures clear accountability, continuous improvement, and compliance with legislative requirements. The Strategic Information Governance Group (SIGG), led by the Senior Information Risk Owner (SIRO), will meet quarterly and oversee delivery by developing an annual action plan that sets out key priorities, milestones, and responsibilities. Progress will be monitored quarterly, with updates provided to the Corporate Management Team (CMT).

To ensure effective delivery, we will take the following practical steps:

- **Governance & Oversight:** The SIGG will meet regularly to review implementation progress, assess emerging risks, and update policies and procedures where needed. The group will also manage compliance with external audits and regulatory requirements.
- **Risk Management:** We will proactively identify, assess, and mitigate risks related to information governance, records management, cybersecurity, and data protection. This includes conducting regular risk assessments and ensuring that high-risk areas receive focused attention.
- **Policy & Framework Development:** A structured framework of policies, procedures, and guidance documents will be maintained and updated to reflect changes in legislation, emerging technologies, and best practices.
- **Training & Awareness:** A continuous training program will be implemented to ensure staff understand their responsibilities and stay informed of any legal or procedural changes. This will include e-learning modules, workshops, and targeted training for key roles such as Information Asset Owners (IAOs).
- **Incident Management & Reporting:** A formal process will be in place to manage data breaches, security incidents, and compliance issues. Lessons learned from incidents will be used to strengthen policies and staff training.
- **Data Quality & Management:** We will ensure that information is accurate, up-to-date, and accessible by developing a data quality framework, maintaining an information asset register, and conducting regular audits.
- **AI & Emerging Technology Governance:** As AI and data analytics become more integrated into council services, we will establish clear guidelines to ensure their ethical, transparent, and compliant use.
- **Performance Monitoring & Continuous Improvement:** Key performance indicators (KPIs) will be developed to measure the effectiveness of our information governance practices. Regular reviews will help identify areas for improvement and ensure alignment with organisational objectives.

By embedding these practical steps into our operations, we will ensure that Information Governance remains a core function of Midlothian Council, supporting compliance, efficiency, and service improvement.

7.0 Summary

7.1 Midlothian Council's Information Governance Strategy 2025-2028 provides a comprehensive framework to protect data assets, comply with legal requirements, and enable innovation.