Information Governance Policy

Implementation date [date policy comes into force as this may differ from approval date]

Control schedule

Approved by	Name of Committee
Approval date	Date of Committee Meeting
Senior Responsible Officer	Andrew Kerr, Chief Executive
Author	Kevin Wilbraham, Information Governance Manager
Scheduled for review	Should be annual – please insert month and year only [as actual date will depend on committee schedule]

Version control

Version	Date	Author	Comment
1.1	09.09.2014	Kevin Wilbraham	Policy issued
1.2	09.09.2016	Kevin Wilbraham	Minor revision to reflect organisational change
1.3	06.07.2019	Kevin Wilbraham	Minor change to reflect legislative change
2.0	21.01.2021	Kevin Wilbraham	Revisions made to incorporate additional policy statements

Date	Committee	Link to report	Link to minute
03.09.2014	Corporate Policy & Strategy		
04.10.2016	Corporate Policy & Strategy		
06.08.2019	Policy & Sustainability		

Policy statement

1.1 The Council obtains, creates and manages a large amount of information relating to its services, customers and partners. This policy sets out the Council's approach and commitment to the effective and lawful management of Council information through good information governance. It also sets out the roles and responsibilities of all stakeholders involved in handling and managing Council information.

Scope

2.1 This policy applies to:

2.1.1 All information held, maintained and used by the Council in all locations and in all media (hardcopy and electronic);

2.1.2 Elected Members, Council staff, including temporary staff, contractors, consultants and volunteers that access and use Council information; and

2.1.3 All third parties that manage and process information on the Council's behalf when carrying out a statutory Council function or service.

Definitions

3.1 The definitions below concern specific terms and descriptions used in this policy. A wider glossary of IG terms is available on the Council's intranet.

Archives: records which are retained permanently because of their continuing business, evidential or informational value to the Council or communities it serves.

Assurance: those processes and functions within the Council that monitor and report on business activity to ensure they are compliant with policy, regulatory and legislative requirements.

Business Classification Scheme: an outline of Council business based on function and activity rather than organisational hierarchy – focusing more on what is done than who does it. It is used to classify Council records and data so that information governance controls can be consistently applied, independent of organisational change.

Controls (organisational): are measures that instruct and define responsibilities and expected behaviours and practices (e.g. policies, procedures, guidance);

Controls (technical): are measures that limit and define access and action via network and system configuration (e.g. account and permissions management, encryption, firewalls and retention and disposal functionality)

Council Records (also Public Records): are those documents created, collected, processed, and used by Council employees, Elected Members when undertaking Council business, predecessor bodies (e.g. Lothian Region Council, Edinburgh District Council, Edinburgh Corporation) or third parties performing a statutory Council function or service, which are then kept as evidence of that business. They can be in any format (including paper, microform, electronic and audio-visual formats).

Data Breach: is a failure in compliance with data protection principles. A breach can occur when an organisation does not manage the confidentiality, integrity, and availability of personal data in compliance with data protection legislation.

Data Controller: a legal person or organisation who determines the purposes for which, and manner in which, personal information is to be processed. This may be an individual or an organisation. Data Controllers can process personal data jointly with other data controllers for specified purposes. The City of Edinburgh Council is a data controller. Elected members are data controllers for the purposes of their constituency work.

Data Protection Impact Assessment: a risk management tool that reduces the risks of harm to individuals through the misuse of their personal information and can help with the design of processes for handling personal data. It is used when projects, or changed service activities, or new ICT impact on the privacy of individuals.

Data Quality: data is the raw input from which information of value is derived. Data quality is a recognition that the accuracy, coverage, timeliness and completeness of data can significantly impact on the value of its use.

Information Asset: a body of information defined and managed as a single unit or aggregate so it can be understood, shared, protected and exploited effectively.

Information Asset Owners: senior officers involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

Information Asset Register: a governance tool that lists the Council's key information assets.

Information Security: is the organisational function that ensures Council information is not compromised by unauthorised access, modification, disclosure or loss.

Open Data: data that is accessible (usually via the internet), in a machine-readable form, free of restriction on use. It supports transparency and accountability, effective services and economic growth.

Personal Data: is information about a living individual who can be identified from that information or from additional information held, or obtained, by the Council. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

Records Management: is the organisational processes and practices that ensure Council records are systematically controlled and maintained, covering the creation, storage, management, access, and disposal of records, in compliance with best practice, legal obligations and policy requirements.

Records Management Plan: a requirement of the Public Records (Scotland) Act, 2011, it is a document created by a Scottish public sector organisation, which outlines its records management arrangements and commitments to improvement, that has been approved by the Keeper of the Records of Scotland.

Policy content

Information is both a major asset and responsibility of the Council

4.1. Information is central to the Council's business processes, decision making, service delivery, and provides evidence and accountability concerning Council actions and performance.

4.2 It is crucial that the information Council staff obtain, create and manage concerning our services, customers and partners is managed effectively to maximise its value and to stop it becoming a liability and a risk.

4.3 This places significant demands on the Council as a Scottish Local Authority. There is a wide-ranging and complex legal landscape in which it has to operate in, which is monitored through various external regulators, including the Scottish Information Commissioner and the UK Information Commissioner.

4.4 The policy's appendix sets out the many acts, regulations, codes of practice and technical standards that are relevant to how the Council manages its information.

Information governance provides the Council with the tools to manage its information effectively and appropriately

4.5 To operate lawfully and effectively within this landscape, the Council needs robust and effective controls and assurances around the management of its information.

4.6 As an organisational function, information governance provides a coherent approach and structure to these controls and assurances. It covers:

- Archival preservation and access
- Records classification, integrity, retention, and disposal
- Personal data processing
- Statutory access to information, including freedom of information, subject access requests, re-use of public sector information and open data
- Data quality management
- Information security

The Council's Information Governance Framework outlines what compliance should look like and supports Service Areas in achieving it

4.7 The Council will develop and maintain an **Information Governance Framework** of necessary policies, standards, procedures and guidance. These will support staff in directing them how to meet their legal, regulatory and ethical obligations around the information they are responsible for.

4.8 Council staff are expected to be aware of and follow these documents, where they are relevant to their work; incorporating their requirements into their day to day practices and processes.

4.9 Aside from this **policy**, the Council will produce and maintain subsidiary **standards** that will outline expected behaviours and models of compliance that Service Areas must work towards implementing, where they are relevant.

4.10 Supplementary **guidance** will also be produced and maintained that will guide Service Areas in how to implement these standards, in part or whole.

4.11 There will be formal **procedures** that govern how Council staff follow organisation-wide information governance processes.

Key Council-wide Requirements

4.12 To comply with its obligations, the Council as an organisation must also:

- Answer statutory requests for information in a timely, comprehensive and transparent manner
- Create and maintain an Information Asset Register and Business Classification Scheme
- Create, publish and maintain a Records Management Plan
- Create, publish and maintain a Publication Scheme
- Consider and allow, where possible, requests to re-use public sector information and identify and publish open data sets
- Establish and maintain reporting processes to ensure that all personal data and information security breaches are reported, investigated, resolved or escalated

- Implement and maintain an information security management system to protect Council information
- Register with the UK Information Commissioner's Office as a Data Controller
- Retain its public records in line with its Record Retention Rules and dispose or transfer them to archival custody in an authorised and documented fashion
- Maintain and provide access to a Council archive for corporate records required for permanent preservation and other non-Council collections in its possession
- Produce accurate, reliable, relevant and timely data
- Undertake Data Protection Impact Assessments for all major changes to how it processes personal data
- Create and maintain a Record of Processing of personal data

Risk management is the means to appropriately manage non-compliance with information governance requirements

4.13 Where Council Service Areas cannot meet relevant standards or the key requirements, managers must record non-compliance as risks within their service and project risk registers, as per the Council's **Risk Management Framework**.

4.14 The Council's **Senior Information Risk Owner** will be the main focus for the assessment and management of information risks, with reporting to the Information Board and Council Leadership Team as appropriate.

The Council's Information Board will advocate, coordinate and monitor efforts to improve information governance within Service Areas

4.15 An Information Board will be established and maintained to own the Council's ambition to continually improve and update its information governance controls and assurances.

4.16 It will be chaired by the Senior Information Risk Owner of the Council and have the following membership:

- Chief Digital Officer
- Chief Risk Officer
- Council Data Protection Officer
- Digital Innovation Manager
- ICT Enterprise Architect
- Change and Delivery Manager (Performance and Data)
- Representative from the Health and Social Care Partnership
- Representative from Communities and Families
- Representative from Resources
- Representative from Place

4.17 It will advocate, co-ordinate, promote, monitor and assure the development and delivery of information governance improvements and processes. This activity will be driven through the board's **Annual Forward Plan**.

4.18 Specific issues and progress will be presented to the Information Board as a matter of routine and highlighted to the Council Leadership Team and Elected Members when required.

4.19 Co-ordination, advocacy and the management of risks concerning cyber-security and information-security are under auspices of the Cyber Information Security Steering Group.

Implementation

5.1 The policy will be implemented and monitored through the Information Board's Annual Forward Plan, as described above. The plan will set out key tasks, outcomes, accountabilities and progress.

5.2 A key part of this policy will be the suite of subsidiary information governance standards, which will set out what is expected of Council Service Areas in a range of compliance areas. Their development, maintenance and adoption throughout the Council will be essential.

5.3 The Council will also provide training resources at different levels and on different topics to its staff to ensure that they are aware of what is required of them from this policy and its standards.

5.4 Regular communications will be distributed to Council staff to highlight specific issues or events as well as sources of help. These will be agreed by the Information Board and through the Communications Service to ensure that they are effective, relevant, and targeted at the right audience.

Monitoring compliance and measuring success

5.5 Many elements of information governance have key performance indicators in place to ensure service delivery meets statutory requirements (e.g. freedom of information and data protection). However, it also contains elements that are less tangible to measure, such as cultures and behaviours.

5.6 To provide a more complete measure of success and improvement, the Council will undertake an annual **information governance maturity assessment** to determine compliance with and progress against its Information Governance Framework.

5.7 The results of the annual assessment will be presented to the Information Board and directorates and will be used to inform themes and work priorities for the Information Board's following Annual Forward Plan.

Roles and Responsibilities

6.1 Everyone covered by this policy has a responsibility for managing Council information appropriately and lawfully. However, there are specific role responsibilities which are required to ensure that the Council has the right leadership, expertise, ownership and accountability concerning the management of information. These specific roles and responsibilities are set out below.

Council Leadership Team

6.2 The Chief Executive and Executive Directors have overall collective responsibility for information governance compliance and performance within the Council.

This involves:

- providing high-level support to ensure that each directorate applies relevant policies and adopts relevant standards:
- providing evidenced statements of information assurance as part of the Council's annual governance statement: and
- fostering a culture of innovation, responsibility and transparency that values and invests in Council information assets for the benefit of Edinburgh and its citizens

Senior Information Risk Owner

6.3 The Democracy, Governance & Resilience Senior Manager is the Council's Senior Information Risk Owner (SIRO). The SIRO provides a focus for the assessment and management of information risks across the Council.

Specific responsibilities include:

- Owning the organisation's overall information risk assessment processes and ensuring they are implemented consistently.
- Ensuring information risks are managed and reported as appropriate within the Council's risk management framework.
- Providing the final point of resolution for any information risk issues.
- Chairing the Information Board, which will be responsible for promoting, monitoring and assuring the development and delivery of effective information management within the Council.

Data Protection Officer

6.4 The Information Governance & Strategic Complaints Manager is the Council's Data Protection Officer (DPO). The DPO is responsible for monitoring and promoting compliance with data protection law.

Specific responsibilities include:

- Acting as the first point of contact for members of the public and the UK Information Commissioner's Office in relation to data protection matters.
- Providing data protection support and advice to Council services
- Monitoring compliance with data protection law and associated Council standards, protocols and processes
- Providing advice on privacy risks by supporting the competition of data protection assessments

Senior Manager, Operational Records Manager and Archive Responsibilities under the Public Records (Scotland) Act, 2011

6.5 The Chief Executive is the Senior Manager responsible for the management of the Council's public records and its statutory Records Management Plan.

6.6 The Council's Information Asset Manager is the Operational Records Manager responsible for implementing and updating the Council's statutory Records Management Plan. They are also responsible for the transfer, preservation and use of the Council's records as archives, as well as other archives in Council custody.

Information Asset Owners (IAOs)

6.7 IAOs are heads of service who are accountable for the **information assets** within their service area, or those information assets across the Council that supports the corporate function (e.g. HR, Finance, Property) they are responsible for.

6.8 They are responsible for ensuring that staff manage information appropriately, in line with the Council's information governance standards and procedures, and that **information risks** are properly identified and managed.

Information Governance Unit (IGU)

6.9 The IGU is responsible for the creation, publication and maintenance of the Council's **Information Governance Framework**.

6.10 It is also responsible for the daily operation of many of the information governance controls, assurances and processes within the Council.

Specific responsibilities include:

- Developing and driving information governance standards and practices across the organisation
- Assessing and highlighting information governance maturity, compliance and performance
- Providing a focal point for all information governance enquiries
- Assessing and mitigating information risks through data protection assessments, breach reporting and performance assessments

- Upholding the information rights of citizens by responding to statutory requests for information, and other rights defined in legislation
- Preserving and providing access to the Council's archives
- Liaising with external regulators on information governance issues
- Supporting digital working across the organisation
- Providing training resources for staff and ensuring appropriate levels of awareness around information governance matters

Information Board

6.11 The Information Board owns and drives the broader information management agenda throughout the Council. It will support, co-ordinate, promote, monitor and assure the development and delivery of information governance improvements within the organisation.

6.12 It is responsible for effective information risk management within the Council, providing a level of assurance to the Council's Corporate Leadership Team that appropriate frameworks and initiatives are in place to ensure Council information is used and managed effectively and compliantly.

Cyber Information Security Steering Group

6.13 The Cyber Information Security Steering Group provides a forum for improving Council wide governance and risk management around cyber-security and information-security issues more generally. It promotes compliance with the Council's Information Security Management Strategy and actively manages risks to ensure the safe and secure use of all ICT Systems and information in line with legislation, good practice and the requirements of the Public Sector Action Plan for Cyber Resilience.

Managers and supervisors

6.14 All managers and supervisors have a responsibility for enabling and promoting effective information governance within their respective service areas and teams. This includes, but is not limited to:

- Ensuring that information governance standards, procedures and guidance are understood and followed
- Integrating information governance standards into local processes to ensure that there is on-going compliance on a day to day basis
- Reporting any suspected personal data breaches or information loss
- Identifying and reporting any information risks relating to their service area
- Carrying out information governance assessments when required

All employees

6.15 Managing information effectively and lawfully is the responsibility of everyone. Individuals must ensure that they are familiar with the Council's information

governance standards, processes and guidance, and take appropriate care when receiving, creating, using, sharing and disposing of information in the course of their work.

Related documents

7.1 The policy's appendix sets out the many acts, regulations, codes of practice and technical standards in relation to information governance.

Integrated impact assessment

8.1 An integrated impact assessment was carried out and no specific concerns were highlighted.

Risk assessment

9.1 The risks of not implementing this policy include:

- Distress or harm to individuals or organisations.
- Reputational damage to the Council.
- Financial loss or monetary penalty imposed.
- Detrimental impact on Council business and service delivery.
- Non-compliance with legislation and potential litigation.

Review

10.1 This policy will be reviewed annually or more frequently if required by significant changes in legislation, regulation or business practice. It will be reviewed by the Information Board and presented to Council committee annually, in line with the Council's Policy Framework.

Appendix

Key documents in relation to Scottish local government and the management of information are detailed below:

Key Acts of the UK Parliament

1973 c.52 Prescription and Limitation (Scotland) Act 1973

1973 c.65 Local Government (Scotland) Act 1973

1985 c.43 Local Government (Access to Information) Act 1985

1990 c.18 Computer Misuse Act 1990

1994 c.39 Local Government etc. (Scotland) Act 1994

1998 c.29 Data Protection Act 2018

Key Acts of the Scottish Parliament

2002 asp. 13 Freedom of Information (Scotland) Act 2002

2003 asp. 01 Local Government in Scotland Act 2003

2011 asp. 12 Public Records (Scotland) Act 2011

2014 asp. 09 Public Bodies (Joint Working) (Scotland) Act 2014

Key Statutory Instruments of the UK Parliament

S.I. 2015 / 1415 The Re-use of Public Sector Information Regulations, 2015

Key Statutory Instruments of the Scottish Parliament

S.S.I. 2003 / 581 The Pupil's Educational Records (Scotland) Regulations

S.S.I. 2004 / 520 Environmental Information (Scotland) Regulations

Key Statutory Codes of Practice

Section 60 Code of Practice: Function under FOI(S)A

Section 61 Code of Practice: Records Management and FOI(S)A

Key International & British Standards

ISO 15489: 2001 Information and Documentation - Records Management

ISO 16175 Principles and functional requirements for records in electronic office environments

ISO 23081 Metadata for records

ISO 27000 series – Information Security Management System

ISO 30300 series – Management Systems for Records