# Corporate Policy and Strategy Committee

**10am, Tuesday, 30 September 2014**

# Information Governance Policies

| | |
|---|---|
| **Item number** | 7.4 |
| **Report number** | |
| **Executive/routine** | |
| **Wards** | All |

## Executive summary

Information is a key asset for the Council. It needs to be managed effectively to maximise value for the Council and its stakeholders, and to manage related risks.

The Council has developed an Information Governance Strategy. A framework is now being developed as part of this Strategy to help services manage their information more effectively and to mitigate information risks.

The development of this suite of Information Governance policies detailing responsibilities and requirements helps ensure compliance with legislative, regulatory and best practice standards.

## Links

| | |
|---|---|
| **Coalition pledges** | |
| **Council outcomes** | |
| **Single Outcome Agreement** | |

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

# Report

## Information Governance Policies

### Recommendations

1.1 To note the Information Governance Strategy set out in appendix 1 of this report; and

1.2 To approve the Information Governance policies set out in appendices 3 to 7 of this report.

### Background

2.1 Information is a key asset for the Council. It is central to the Council's business processes, decision making and service delivery. It also provides evidence and ensures accountability for Council actions and performance. It is crucial that information is managed effectively to maximise value for the Council and its stakeholders, and to manage related risks.

2.2 The effective management of information places significant demands on the Council. In particular, there is a wide ranging, dynamic and complex legal landscape in which the Council has to operate. Appendix 1 (part A) details the principal acts, regulations, codes of practice and technical standards concerning information governance.

2.3 Compliance with this range of legislation is monitored through various external regulators, including the Scottish Information Commissioner and the Information Commissioner. The latter, in particular, has a wide range of enforcement powers if organisations are found to breach the Data Protection Act. These include powers to impose monetary penalties of up to £500,000 for each breach. The number of organisations, including local authorities, receiving monetary penalties has continued to increase in 2013-14. (http://ico.org.uk/enforcement/fines)

2.4 In March 2015, the Information Commissioner's Officer (ICO) will undertake a voluntary audit of the Council's arrangements for complying with the statutory requirements of the Data Protection Act 1998 and best practice guidance issued by the ICO. This will involve a comprehensive review of the Council's protection policies, procedures and processes, including how these are followed and quality assurance within the Council.

2.5 The Council will not be subject to any enforcement actions resulting from any non-compliance or breaches of the legislation discovered through the audit process. However, where compliance issues and shortcomings are identified,

the ICO will conduct a follow-up audit to ensure that improvement actions have been implemented.

2.6 To help prepare for the ICO audit and to ensure the efficient and effective management of Council information, an Information Governance strategy, outlined in appendix 1, has been developed and agreed with the Corporate Management Team (CMT).

2.7 Information Governance provides a coherent approach and structure that brings together all the legislative and regulatory requirements, standards and best practice in relation to data quality; information compliance (including data protection and freedom of information); information security; information sharing; open data; and records management. Overall, it ensures that the Council is creating, managing, using, sharing and disposing of information efficiently, appropriately and lawfully.

2.8 A key element of the Information Governance Strategy is the establishment of an Information Council to provide the necessary ownership and advocacy function to support, co-ordinate, promote, monitor and assure the development and delivery of effective information governance.

2.9 The Information Council is leading the development of an information governance framework for the Council. The framework consists of policies, standards, guidance and tools including details about how they will be implemented, measured and assured. The framework will provide the Council with a coherent structure to ensure that legal and best practice standards are met and continuously assessed.

## Main report

3.1 Each Information Governance area has a top level policy, outlined in paragraphs 3.4- 3.8 below. Each policy clearly sets out roles, responsibilities and requirements to ensure compliance with legislative, regulatory and best practice standards.

3.2 All policies will be available on the Council's Policy Register and reviewed on annual basis by CMT and Committee.

3.3 Policies concerning Information Security and Open Data are covered through the Council's ICT Acceptable Use Policy and the Open Data Strategy respectively. Information sharing which is mostly concerned with the sharing of personal information is included as part of the Data Protection Policy.

**Information Governance Policy** (Appendix 2)

3.4 This policy formalises the Council's overall approach to information governance by detailing the various elements of the Information Governance framework, and

the methodology that will be adopted and developed to ensure compliance with that framework.

**Data Protection Policy** (Appendix 3)

3.5 This policy sets out and formalises the Council's approach for ensuring that personal information is properly processed, managed and protected in accordance with the requirements of the Data Protection Act 1998. It outlines the Council's commitment to the principles enshrined within the Act and the need to balance the rights of individuals with the functions and operational requirements of the Council.

**Data Quality Policy** (Appendix 4)

3.6 This policy confirms the Council's commitment and approach to improving the quality of its data. It sets out a number of key principles around data collection, management and presentation. The policy recognises that the Council needs reliable, relevant, accurate and timely data to facilitate service delivery and improvement and to account for its performance.

**Freedom of Information Policy** (Appendix 5)

3.7 This policy formalises the Council's approach to the management and release of information in accordance with the provisions of the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, and the INSPIRE (Scotland) Regulations 2009. It sets out the Council's commitment to openness, transparency and accountability and to up-holding the information rights of individuals.

**Records Management Policy** (Appendix 6)

3.8 This policy sets out the baseline requirements and actions for effective records management, ensuring that records properly support and underpin the effective operation and management of the Council, including compliance with the Public Records (Scotland) Act 2011.

**Procedures and guidance**

3.9 Corporate procedures and guidance have been developed and made available on the ORB to support staff in implementing and complying with agreed policies. These will be revised and communicated on a regular basis to reflect any changes in legislation, standards and best practice. Where appropriate, local procedures will also be developed or quality assured by the Council's Information Governance Unit to reflect local needs and conditions.

**Training**

3.10 Training, education and awareness are essential to ensure compliance with policies and procedures, as well as promoting a culture of corporate responsibility that values information as an asset.

3.11 A training programme and series of awareness raising sessions have been scheduled over the next 12 months to ensure that all staff are aware of their responsibilities in using and managing Council information. The programme will be delivered at an appropriate level to all staff using e-learning and other delivery mechanisms.

3.12 Training on this suite of policies, once agreed, will also form part of the Council's key mandatory policy awareness programme, and will be a mandatory component of the Council's induction process for all new staff, going forward.

## Measures of success

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

4.2 To provide a more complete measure of success and improvement, an information governance maturity assessment will be developed to determine progress on an annual basis against the Council's Information Governance Framework and associated policies.

## Financial impact

5.1 Failure to comply with the requirements of the Data Protection Act 1998 could result in enforcement action by the Information Commissioner's Office, including imposition of a civil monetary penalty that could result in a fine of up to £500,000 for each breach.

5.2 Failure to identify and apply appropriate retention rules to Council records could result in excessive and unnecessary physical and IT storage costs.

## Risk, policy, compliance and governance impact

6.1 Impacts could be severe, including: distress or harm to individuals or organisation; reputational damage to the Council; detrimental impact on Council business and service delivery; and non-compliance with legislation and potential litigation.

## Equalities impact

7.1 There are no adverse equalities issues arising from this report.

## Sustainability impact

8.1 There are no sustainability issues arising from this report.

## Consultation and engagement

9.1 The suite of policies has been developed in consultation with all service area representatives across the Council who are members of the Information Council.

## Background reading/external references

Public Records (Scotland) Act 2011

Freedom of Information (Scotland) Act 2002

Environmental Information (Scotland) Regulations 2004

INSPIRE (Scotland) Regulations 2009

Data Protection Act 1998

Office of the Scottish Information Commissioner

Information Commissioner's Office

**Alastair Maclean**

Director of Corporate Governance

Contact: Kirsty-Louise Campbell, Governance Manager

E-mail: kirstylouise.campbell@edinburgh.gov.uk | Tel: 0131 529 3654

Contact: Kevin Wilbraham, Records & Information Compliance Manager

E-mail: kevin.wibraham@edinburgh.gov.uk | Tel: 0131 469 6174

## Links

**Coalition pledges**

**Council outcomes**

**Single Outcome Agreement**

**Appendices:**

Appendix 1 – Information Governance Strategy
Appendix 2 – Information Governance Policy
Appendix 3 – Data Protection Policy
Appendix 4 – Data Quality Policy
Appendix 5 – Freedom of Information Policy
Appendix 6 - Records Management Policy

**Appendix 1 – Information Governance Strategy**

## Introduction

Information is a key asset for the Council. It is at the centre of the Council's business processes, informs and shapes decision making, helps with the delivery of quality customer services, provides evidence and accountability of our actions, and lets us know how we are performing.

Like any other asset, such as property, finance and people, information has to be managed effectively to stop it becoming a liability and risk, and to ensure we can maximise its value for the Council and our stakeholders. Failure to manage information appropriately can lead to reputational loss and considerable financial penalties.

The effective management of information places significant demands on the Council. In particular, there is a wide-ranging and complex legal landscape within which the Council has to operate. Appendix 1A details the many acts, regulations, codes of practice and technical standards concerning information governance.

## Vision

To operate effectively within this landscape the City of Edinburgh Council needs to:

- Embed a culture of confidence and responsibility in managing information to provide a consistent and improved service for our customers;
- Provide clear leadership, training and awareness to empower all staff to handle information effectively and to identify opportunities for improvement and transformation; and
- Ensure the Council's information governance arrangements are continuously assessed, co-ordinated, improved and assured to manage risk, meet compliance standards and drive efficiencies.

## How do we do this?

To achieve this we need effective information governance. Information Governance is the assurance we have as a Council that we are managing our information efficiently, appropriately and lawfully. This includes how we create, manage, use, share, and dispose of information, incorporating the areas of:


Definitions:

| | |
|---|---|
| **Data quality** | Ensures that the Council's information is accurate, reliable, relevant and up-to-date. |
| **Information security** | Ensures that Council information is not compromised by unauthorised access, modification or loss. |
| **Information compliance** | Ensures compliance with all legislation that is relevant to the management of information, including rights of access under freedom of information and data protection legislation. |

| | |
|---|---|
| **Records management** | Ensures that Council information is systematically controlled and maintained, and includes arrangements for storing, managing, accessing, using and disposing of records, in compliance with legal and policy requirements. |
| **Information sharing** | Ensures that Council information is shared in a secure and controlled manner. |

## Information Council

While managing information is the responsibility of all staff, an Information Council has been established to provide the necessary ownership and advocacy function to support, co-ordinate, promote, monitor and assure the development and delivery of effective information governance.

The Information Council will consist of senior officers representing all directorates of the Council, ICT Solutions and those with corporate responsibilities for information governance. The Council will be chaired by the Council's Governance Manager who will report to the Director of Corporate Governance (who is designated as the Council's Senior Information Risk Owner), the Council Management Team and Elected Members.

The Information Council will:

- Provide strategic leadership for information governance and information risk management throughout the Council.
- Support the development of the Information Governance Framework, including an annual maturity assessment to measure progress and improvement.
- Support, monitor and approve the annual information governance improvement plan, including plan revision and realignment to mitigate risk.
- Take ownership of the information risk management approach, including monitoring compliance with the Information Governance Framework and highlighting information risks.
- Receive and consider reports into breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.
- Develop solutions and implementation programmes to ensure that the Council complies with developing information governance requirements.
- Support directorates with the implementation of information governance standards, policies and controls.
- Support audit and assessment arrangements for information governance.

- Ensure that Council's approach to information governance and information risk is effective in terms of resource, commitment and execution.
- Create, direct and support subsidiary Council groups (e.g. Data Council) in developing, maintaining and complying with the Information Governance Framework.
- Liaise with other working groups and programme boards to ensure compliance with the Council's Information Governance Framework.
- Provide a focal point for the resolution and/or discussion of information governance issues.

## Information Governance Framework

A core activity of the Information Council and a central part of this strategy is the establishment of an information governance framework. This will provide the Council with a robust and coherent structure to realise the information governance vision, as well as ensuring that legal requirements and best practice standards are met.

The framework forms part of the Corporate Governance Service Plan and will consist of policies, standards, guidance and tools, and details about how they will be implemented and assured.

## Information Governance Action Plan

The Information Governance Framework and wider strategy will be delivered through an Action Plan. This will be approved and monitored by the Information Council on an annual basis. The Plan will include policy, guidance and tools development, as well as assessments, feedback and regular communications. The Plan will be flexible enough to incorporate risk mitigation, transformation programmes and business improvement opportunities, ensuring that resource can be directed to where it is most needed.

## Information risk management

There are significant risks to the Council if information is not managed properly. The Information Governance Framework will build on the corporate risk approach to ensure that information risks are identified, assessed and managed. In particular, the delivery of training, education and awareness will be required to ensure staff can identify and treat information risks.

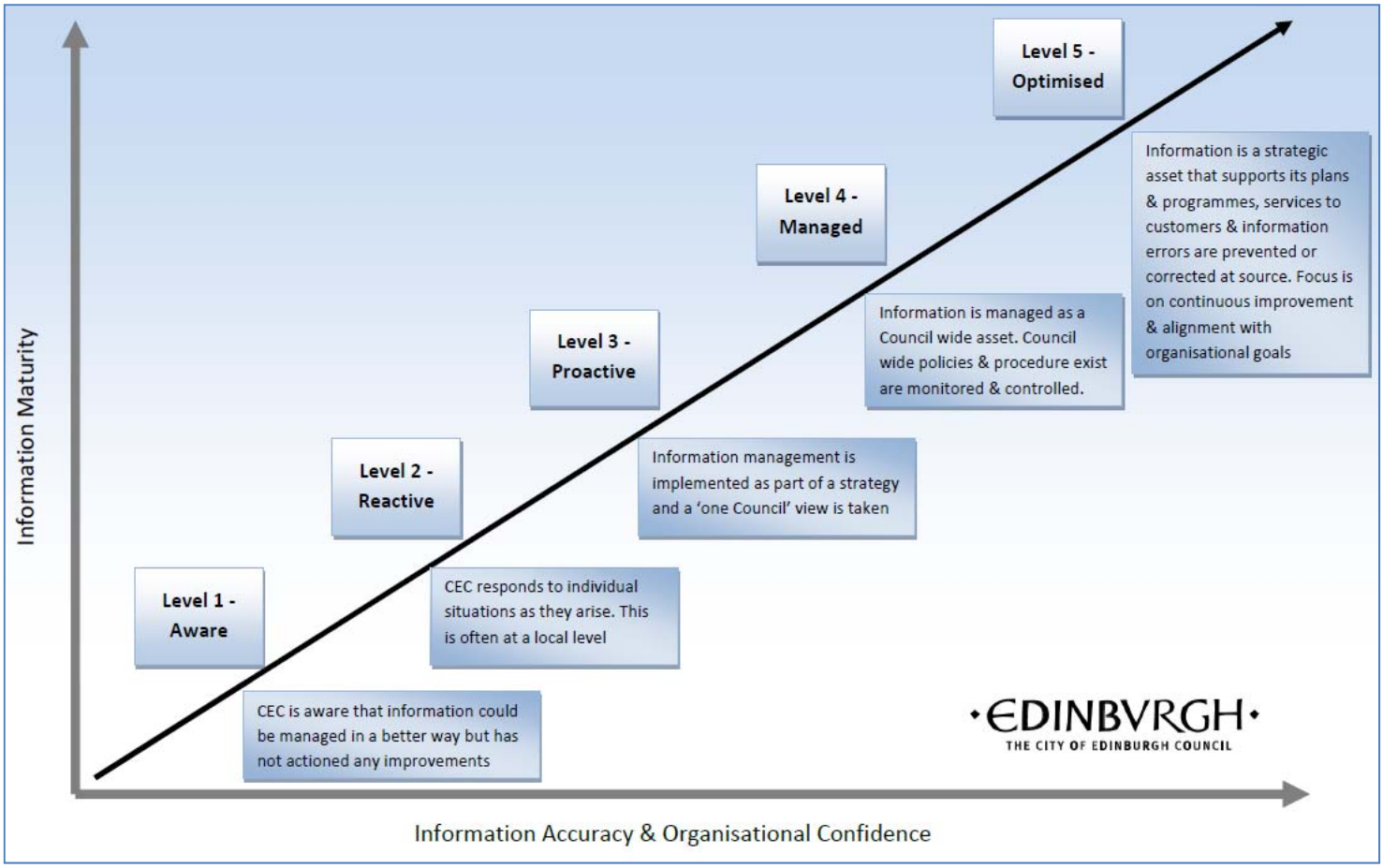
## How will this be measured?

All the projects and areas of work required to deliver this strategy will have performance measures in place to ensure delivery meets quality requirements in line with the action plan. Progress will be presented to the Information Council as a matter of routine, and regularly highlighted to the Council Management Team and Elected Members.

This strategy also contains elements which are less tangible to measure such as cultures and behaviours. To provide the Council with a more complete picture of what effective information governance should look like, an Information Governance Maturity Model will be used to determine progress against this strategy. Overall success will be determined by improvement in maturity and evaluated over a five year period.

A detailed model will be developed as part of this strategy and based on the UK Government's Information Assurance Maturity Model.

**Information Governance – Basic Maturity Model**



## Responsibilities

Overall responsibility for delivery of this strategy will lie with the Governance Manager with support from the Information Council. However, to implement the Council's vision for information governance, everyone from front line staff to senior managers must understand their role and responsibilities when managing Council information. This will help to create clear lines of leadership and accountability, as well as promoting a corporate culture where information is valued and assured.

Specific responsibilities will be clearly highlighted in the policy documents that will form part of the Information Governance Framework.

## Appendix 1A – Information Legislation

Information management underpins all European, UK and Scottish legislation, regulation and guidance that affects, directs or empowers the City of Edinburgh Council. As a result, a definitive list of all such relevant legislation, regulations and standards would be too long to be useful here. Key documents, however, in relation to Scottish local government and the management of information management 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 1998 |
| **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 |
| **Key Statutory Instruments of the UK Parliament** |
| S.I. 2005 / 1515 The Re-use of Public Sector Information Regulations, 2005 |
| **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 27001 Information Security Management |
| ISO 30300 & 30301 Management Systems for Records |

| |
|---|
| BS10008 Evidential Weight and Legal Admissibility of Electronic Information |
| 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 |

# Appendix 2 - Information Governance Policy

## Policy statement

1.1 This policy sets out the Council's information governance (IG) framework to ensure that information is effectively managed and properly protected. It also clearly defines the roles and responsibilities of all stakeholders involved in handling and managing Council information.

1.2 The IG strategy provides the overall direction and vision for information governance within the Council, including the development of an IG policy and framework.

## 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 (paper 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 Appendix 2A provides a glossary of terms and definitions commonly used in relation to IG. The definitions below concern specific terms and descriptions used in this policy.

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

3.1.2 **Data Stewards**: individuals with delegated authority to apply IG rules, including the up-dating of Council data and records to ensure data integrity and quality.

3.1.3 **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**.**

3.1.4 **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.

3.1.5 **Information asset owners:** senior officers involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

3.1.6 **Information asset register**: a governance tool that lists the Council's key information assets.

3.1.7 **Information compliance:** ensures compliance with all statutory requirements governing the management of information, including rights of access under freedom of information and data protection legislation.

3.1.8 **Information security**: ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

3.1.9 **Information sharing**: ensures that Council information is shared in a compliant, controlled and transparent manner.

3.1.10 **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.

3.1.11 **Privacy 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.

3.1.12 **Records management:** 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. International Standard ISO15489 covers the fundamentals of good records management.

3.1.13 **Vital records:** records classified as being essential to the continuation of Council business.

# Policy content

4.1 Information is a key asset for the Council. It 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 information is managed effectively to maximise its value for the Council and its stakeholders, and to stop it becoming a liability and a risk.

4.3 IG provides a framework for bringing together all the legislative and regulatory requirements, standards and best practice in relation to the following areas:

4.3.1 Data quality
4.3.2 Information security
4.3.3 Information compliance
4.3.4 Records management
4.3.5 Information sharing

4.3.6 Open data

4.4 It ensures that the Council is creating, managing, using, sharing and disposing of information efficiently, appropriately and lawfully.

4.5 The effective management of information places significant demands on the Council. In particular, there is a wide-ranging and complex legal landscape within which the Council has to operate. Appendix 1A within the Information Governance Strategy details the many acts, regulations, codes of practice and technical standards concerning IG.

**Information governance framework**

4.6 The IG framework provides the Council with a coherent structure to ensure that legal and best practice standards are met and continuously assessed. It consists of the following elements:

**Policies**

4.6.1 Each IG framework area will have a top level policy detailing responsibilities and requirements to ensure compliance with legislative, regulatory and best practice standards. All policies will be available on the Council's Policy Register and reviewed on annual basis by the Information Council and agreed by CMT and Committee.

**Procedures**

4.6.2 There will be documented corporate procedures to support agreed policies which will be developed by the relevant IG area. These will support policy implementation and outline any operational requirements to ensure compliance with legislation and standards. Where appropriate, local procedures will be developed or quality assured by the Information Governance Unit and the relevant business area(s).

**Guidance and training**

4.6.3 Training, education and awareness are essential to ensure compliance with policies and procedures, as well as promoting a culture of corporate responsibility that values information as an asset.

4.6.4 Training will be delivered at an appropriate level to all staff using e-learning and other delivery mechanisms by the relevant information governance area. Specific training requirements identified through the information risk management approach will be included in the Information Council's annual work plan. Training will be developed and delivered by the relevant IG area.

**Communications**

4.6.5 Regular communications will be agreed by the Information Council and through the Communications Service to ensure that key information

governance messages are effective, relevant, and targeted at the right audience.

**Compliance, monitoring and reporting**

4.6.6 The Information Governance Unit will facilitate regular and effective monitoring to support the implementation and assessment of IG practices and behaviours across the Council. Managers will also be expected to carry out IG self-assessments on an annual basis.

4.6.7 Specific issues and progress will be presented to the Information Council as a matter of routine, and highlighted to the Corporate Management Team and Elected Members.

4.6.8 An information governance maturity model will be used to determine progress and overall compliance with IG policies and procedures.

**Information asset register**

4.6.9 The Information Governance Unit will maintain an information asset register for the Council to evaluate and assure compliance with information governance policies and processes, recording and highlighting risk as appropriate. The register will also support wider governance and information activities, including resilience, business intelligence, protective marking and open data initiatives.

**Information risk register**

4.6.10 The Information Governance Unit will maintain an information risk register for the Council (in alignment with its corporate risk approach) that will record information breaches, incidents and any risks highlighted through compliance and self-assessment audits. The register will be reviewed routinely by the Information Council, who will ensure that these risks are actively controlled, assessed and managed.

**Information incident reporting**

4.6.11 An incident reporting process will be maintained by the Information Governance Unit to ensure that all information breaches are reported, investigated, resolved or escalated. Where appropriate, incidents will be recorded in the information risk register.

**Privacy impact assessments**

4.6.12 Privacy impact assessments must be carried out by managers when projects, or changed service activities, or new ICT impact on the privacy of individuals.

**Information governance maturity model**

4.6.13 An information governance maturity model will be used by the Information Council initially to determine progress against this policy and the information

governance strategy. Overall success will be determined by improvement in information governance maturity over a five year period.

**Annual report**

4.6.14 The Senior Information Risk Owner will present an information governance annual report to Committee at the end of each financial year. The report will outline key issues and risks, and will serve as a base line to evaluate future performance and development.

**Annual action plan**

4.6.15 The Information Council will approve and monitor an annual action plan for information governance development and compliance. The plan will outline key tasks, outcomes accountabilities and progress.

# Implementation

5.1 This policy will be implemented through the Information Council's annual action plan, as described above.

# Roles and responsibilities

**Corporate Management Team**

6.1 The Corporate Management Team has overall responsibility for IG. This involves providing high-level support to ensure that each directorate applies relevant information governance policies and controls, and the provision of evidenced statements of information assurance as part of the Council's annual governance statement.

6.2 To facilitate the development and implementation of information governance practices, directors will be asked to nominate/ confirm individuals to sit on corporate groups and to carry out specific responsibilities.

**Senior Information Risk Owner**

6.3 The Director of Corporate Governance is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Corporate Management Team with specific responsibility for information risk and mitigation. Specific responsibilities include:

6.3.1 Leading and fostering a corporate culture that values, protects and uses information for the success of the organisation and benefit of its citizens.

6.3.2 Owning the organisation's overall information risk assessment processes and ensuring they are implemented consistently.

6.3.3 Ensuring Elected Members and the Corporate Management Team are adequately briefed on information governance issues and associated risks.

6.3.4 Owning the organisation's information incident management framework
6.3.5 Providing the final point of resolution for any information risk issues.

**Governance Manager (Deputy Senior Information Risk Owner)**

6.4 Accountability for the on-going strategic development of information governance lies with the Governance Manager within the Legal, Risk and Compliance Division of Corporate Governance. The Governance Manager chairs the Information Council and also deputises for the SIRO as required. The Governance Manager also ensures that the Information Governance Framework is compliant with the Council's overall approach to corporate governance.

**Information Council**

6.5 The Information Council (IC) has delegated responsibility, through the SIRO and the Corporate Management Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure information governance compliance.

6.6 The IC is made up of service area representatives that are suitably senior and/ or with necessary expertise. The work undertaken will be line with IC's terms of reference as detailed at Appendix 2B. The IC reports directly to the SIRO, Corporate Management Team and Committee.

**Information Governance Unit**

6.7 The IGU is responsible for the day to day operation and delivery of information governance within the Council. This includes, but is not limited to:

6.7.1 Collating and responding to requests for information under access legislation.
6.7.2 Co-ordinating, maintaining and developing the information asset register.
6.7.3 Co-ordinating, maintaining and developing the register of information sharing protocols and agreements.
6.7.4 Incident reporting and maintenance of the information risk register, ensuring remedial actions have been undertaken.
6.7.5 Undertaking information governance assessments with service areas.
6.7.6 Providing practical guidance and training for staff, including the development of toolkits.
6.7.7 Leading and supporting compliance issues where appropriate (e.g. Public Services Network or Public Records (Scotland) Act 2011).
6.7.8 Developing local guidance and training for service areas.
6.7.9 Preserving and providing access to the Council's archives.
6.7.10 Implementing and supporting the IC's annual plan.
6.7.11 Liaison with external regulators.

6.7.12 The presentation and analysis of key performance data around information governance.
6.7.13 Management and operation of the Council's records centre.
6.7.14 Providing a focal point for all IG enquiries.
6.7.15 Maintenance of register of record retention and disposal rules.
6.7.16 Development and maintenance of IG maturity through the IG maturity model.

**ICT Solutions**

6.8 ICT Solutions is the operational lead on technical IT risks and is responsible for implementing appropriate technical controls, in line with best practice and compliance frameworks (e.g. the Public Services Network). The service works closely with the IGU to ensure that information governance policies, standards, rules and assurance are properly considered as part of the ICT procurement process.

**Managers**

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

6.9.1 Ensuring that information governance policies, standards and guidance are followed, and that there is on-going compliance on a day to day basis by undertaking annual information governance self-assessments.
6.9.2 Integrating information governance into local processes.
6.9.3 Reporting any suspected breaches of confidentiality or information loss.
6.9.4 Identifying existing or emerging information risks relating to their service area and reporting as appropriate.
6.9.5 Carrying out privacy impact assessments where projects, or changed service activities, or new ICT impact on the privacy of individuals.
6.9.6 Undertaking the role of Information Asset Owners as the use of the Information Asset Register is developed and extended to identify and manage the Council's information assets.

**Staff**

6.10 Managing information effectively and appropriately is the responsibility of all staff. Individuals must ensure that they are familiar with relevant information governance policies, processes and guidance, and compliant with legislative and regulatory requirements.

6.11 As part of their role and remit, individuals may also be nominated as Data Stewards (by Information Asset Owners) with operational responsibility for information assets within their respective service areas. This will involve the application of information governance rules, and the up-dating of Council data and records to ensure data integrity and quality.

# Related documents

7.1 Related documents include:

7.1.1 Information Governance Strategy

7.1.2 Information Governance Policy

7.1.3 Records Management Policy

7.1.4 Freedom of Information Policy

7.1.5 Data Quality Policy

7.1.6 ICT Acceptable Use Policy

7.1.7 Employee Code of Conduct

7.1.8 Open Data Strategy

# Equalities impact

8.1 There are no equalities issues arising from this policy.

# Sustainability impact

9.1 There are no sustainability issues arising from this policy.

# Risk assessment

10.1 The risks of not implementing this policy include:

10.1.1 Distress or harm to individuals or organisations.

10.1.2 Reputational damage to the Council.

10.1.3 Financial loss or monetary penalty imposed.

10.1.4 Detrimental impact on Council business and service delivery.

10.1.5 Non-compliance with legislation and potential litigation.

# Review

11.1 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 Council and presented to Council committee annually, in line with the Council's Policy Framework.

# Appendix 2A; Glossary of Information Governance Terms

**A**

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

**B**

**Business Systems** are databases or other software that create or capture information in relation to Council business. They are primarily used for reference but can be used for workflow or data sharing. Systems that hold information the Council would rely on as evidence should be able to manage their content as records and be **Record Keeping Systems**.

**C**

**Civil Monetary Penalty** – the Information Commissioner has powers to impose Civil Monetary Penalties of up to £500 000 where there has been a serious breach of the requirements of the Data Protection Act 1998.

**Council Records:** are defined as;

- recorded information in any format (including paper, microform, electronic and audio-visual formats),
- which are created, collected, processed, and/or used by City of Edinburgh Council employees, Elected Members when undertaking Council business, predecessor bodies (e.g. Lothian Region Council, Edinburgh District Council, Edinburgh Corporation) or contractors performing a statutory Council function or service
- and which are then kept as evidence of that business.
- **Active Records** are about ongoing Council business and are regularly added to or updated.
- **Closed Records** are about Council business that has concluded and are no longer updated but need to be kept for reasons of reference or evidence.

**Criminal Offences under the Data Protection Act 1998** – In Scotland criminal proceedings for an offence under the Data Protection Act 1998 will be brought only by the Procurator Fiscal. In England, Wales and Northern Ireland proceedings can be commenced by the Information Commissioner. The offences under the Data Protection Act 1998 are:

Processing without a valid Notification;

Failure to advise the Information Commissioner of changes to the Notification;

Failure to comply with an Information Notice;

Failure to comply with an Enforcement Notice;

Unlawfully obtaining or disclosing personal data;

Procuring the disclosure of personal data;

Unlawfully selling personal data; and

Enforced subject access.

**D**

**Data controller –** a legal person or organisation who determines the purposes for which, and the 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 purpose of constituency work.

**Data:** the raw input from which information of value is derived.

**Data Council** has delegated authority through the IC and supports the implementation of the information governance strategy particularly the Data Quality work stream. The Data Council is chaired by the Information Governance Manager. Key responsibilities include:

- Supporting and improving data quality in the Council;
- Supporting the development of guidance and training around data quality; and
- Providing information and guidance on data management processes.

**Data quality:** recognition that the accuracy, coverage, timeliness and completeness of data can significantly impact on the value of its use.

**Data processor –** is a person, other than an employee of the Council, who processes personal data on behalf of the Council. This processing must be evidenced in a written contract. The data processor can only use personal data under the instructions of the Council. The Council retains full responsibility for the actions of the data processor in relation to the personal data.

**Data Protection Act 1998** – gives effect in the UK law to the EC Directive 95/46/EC and came into force on 1 March 2000 repealing the Data Protection Act 1984. The Data Protection Act 1998, together with a number of Statutory Instruments, requires data controllers to comply with the legislation governing how personal data is used for statutory and business purposes. Amendments have also been created by other

legislation such as the Freedom of Information Act 2000. It gives rights to individuals in relation to how organisation can use their personal data.

**Data subject** – a living individual who can be identified from the personal data or from additional information held, or obtained, by the Council. For example, a CCTV image which can identify someone when linked to building access control codes.

**Data stewards** are nominated by Information Asset Owners with operational responsibility for information assets within their respective service areas. This will involve the application of information governance rules, and the up-dating of Council data and records to help ensure data integrity and quality.

**E**

**EIRs** are the Environmental Information (Scotland) Regulations 2004

**Enforcement Notice** – The Information Commissioner has the power to serve an enforcement notice on a data controller if he determines that a data controller has failed to comply with the requirements of the Data Protection Act 1998. The Notice sets out the actions that the data controller must take to achieve compliance. A data controller can lodge an appeal against the Notice to the Information Tribunal. If the data controller fails to comply with a valid Enforcement Notice this is a criminal offence under the Data Protection Act 1998.

**Enforcement Notice** – The Scottish Information Commissioner has the power to serve an enforcement notice where she is satisfied that a Scottish public authority has failed to comply with a Provision of Part 1 of FOISA, the EIRs or INSPIRE. Any Enforcement Notice sets out the actions the Scottish Information Commissioner requires the Scottish Public Authority to take to ensure compliance with the legislation and the timescale for completing these. If the Scottish Public Authority fails to comply with this Enforcement Notice, the Scottish Information Commissioner can refer them to the Court of Session for failure to comply, and the Court of Session may deal with the authority as if it had committed a contempt of court.

**Exception:** This is a regulation under regulations 10 or 11 of the Environmental Information (Scotland) Regulations 2004 which, if applicable to information covered by the request, means that the information does not need to be disclosed.

**Exempt information** is defined as information which does not have to be disclosed in response to an information request because one of the sections in part 2 of the Freedom of Information (Scotland) Act 2002 or Regulations 10 or 11 of the Environmental Information (Scotland) Regulations apply to it.

**Exemption:** This is a section in Part 2 of the Freedom of Information (Scotland) Act 2002 which, if applicable to information covered by the request, means that the information does not need to be disclosed.

**F**

**Files** are collections of records with a connection that are grouped together to be accessed and managed as a single item.

**File Plan** is a governance tool that classifies Council records in terms of Council function and activity; it acts as the baseline to connect this policy, and its related guidance and procedures, to the business processes that create, manage, use and dispose of Council records.

**FOISA** is the Freedom of Information (Scotland) Act 2002

**Format** is the medium is which records are created from; most electronic formats are capable of being edited and changed continually (e.g. MS Word), 'fixed formats' do not allow this (e.g. PDF).

**G**

**General entitlement** means the right of any person, anywhere in the world to make a request for any recorded information held by the Council under the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004.

**H**

**I**

**Information** means any information recorded in any form.

**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 Commissioner** – is responsible for the regulation of the Data Protection Act 1998 throughout the UK. The Information Commissioner is appointed by the Queen and is independent of the UK Government.

**Information compliance:** ensures compliance with all statutory requirements governing the management of information, including rights of access under freedom of information and data protection legislation.

**Information Council (IC)** has delegated responsibility, through the SIRO and the Corporate Management Team, for the development and delivery of effective

information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure information governance compliance.

**Information Governance Framework** is a suite of policies, procedures, guidance and standards covering the following areas; Data Quality, Information Compliance, Information Sharing, Information Security and Records Management.

**Information Notice** – an Information Notice can be issued by the Information Commissioner which requires a data controller to provide his office with information that he requires to carry out his functions. Failure to comply with an Information Notice is a criminal offence.

**Information security:** ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

**Information sharing:** ensures that Council information is shared in a compliant, controlled and transparent manner.

**INSPIRE** means the INSPIRE (Scotland) Regulations 2009

**J**

**K**

**L**

**Limitation:** This is a regulation under regulation 10 of the INSPIRE (Scotland) Regulations 2009 which, if applicable to the information covered by the request, means that the information does not need to be disclosed.

**M**

**Meta data** means information describing spatial data sets and spatial data services and making it possible to discover, inventory and use them.

**N**

**Notification** - the Council is required to Notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. Failure to Notify is a **criminal offence**. The Council must inform the Information Commissioner of any changes to the processing of personal data and renew the Notification annually. Failure to do so is also a **criminal offence**. The Information Commissioner maintains, and publishes, a Register of Data Controllers.

Elected Members are required to lodge, and maintain, a separate Notification to cover constituency work. Failure to do so is a **criminal offence**.

**O**

**P**

**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.

**Practice Recommendation** – The Scottish Information Commissioner may issue a Practice Recommendation to a Scottish public authority where she finds that the authority has not complied with the Codes of Practice issued under sections 60 and 61 of FOISA. Any Practice Recommendation issued by the Scottish Information Commissioner will set out where she considers the Scottish Public Authority not to have complied with the Code(s) of Practice and the action(s) they should take to conform.

**Processing** – is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

**Public interest test** means the consideration that has been given to whether the interests of the public lie in disclosure of the information covered by the request, and that the public interest in disclosing information is not outweighed by that in maintaining the exemption. (FOISA)

That, in all the circumstances, the public interest in making the information available is outweighed by that in maintaining the exception. (EIRs)

That, the public interest in limiting or placing conditions on public access outweighs the public interest in providing full access, in all the circumstances of the case. (INSPIRE)

**Publication scheme** is a guide to the information which the Council routinely makes publicly available.

**Public Records (Scotland) Act 2011:** requires public authorities to detail their records management policies, procedures and responsibilities in a Records Management Plan, which is subject to review by the Keeper of the Records of Scotland. It also requires public authorities to monitor the management of records produced by their contractors undertaking any statutory functions performed on their behalf.

**Q**

**R**

**Records** see **Council Records**

**Record Group**

Records that have the same business purpose can be described as belonging to a record group or series. They do not need to be the same in focus (e.g. different clients, buildings or projects), format (e.g. paper or electronic) or style (e.g. forms, correspondence, reports etc.). Records belonging to the same group have the same retention rule. Record groups can be either Common or Service Specific;

- **Common Record Groups** are created and used by more than one service area of the Council (e.g. Financial Transactions)
- **Service Specific Record Groups** are created by a single service area of the Council (e.g. Building Warrants)

**Record keeping systems**

Council business systems that hold electronic records must be configured to ensure they create, maintain and dispose of those records in compliance with statutory requirements and professional standards. The Council's Information Management Group is responsible for issuing and maintaining **guidance** on electronic record keeping systems to support managers in acquiring and using appropriate systems.

**Records management:** are the 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. International Standard **ISO15489** covers the fundamentals of good records management.

**Records Management Manual** – a document that details how records are created, maintained and disposed of within a team, service area, project or working group.

**Records Series** see **Record Group**

**Requirement for review** means a written request to the Council expressing dissatisfaction with its response to an information request, asking it to review its actions and decision(s) in relation to the request.

**Retention Rules** identify when closed records or files can be disposed of and what should happen to them at that point. They can be broken down into four parts;

- Activity / Record Description – *provides the context on what is covered by the retention rule*
- Trigger – *indicates the moment that the retention period starts applying; usually around the event or date that "closes" a record*
- Retention Period – *how long you hold onto a record beyond the trigger point*
- Disposal Action – *the action required once a record has reached the end of its retention period*

**Retention Schedule** is a collection of authorised retention rules, usually grouped together by function and activity.

**S**

**Scottish Information Commissioner –** is responsible for the promotion and enforcement of the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009 and any associated Codes of Practice.

**Sensitive Personal Data** – requires a higher level of consideration. The following categories are defined as 'sensitive personal data' for the purposes of the Data Protection Act 1998 –

Racial or ethnic origin of the data subject;

Political Opinions;

Religious or similar beliefs;

Trade Union membership;

Physical or mental health or condition;

Sexual life; and

Criminal offences or alleged criminal activity (and any criminal proceedings).

**Spatial Data** means any data with a direct or indirect reference to a specific location or geographical area.

**Spatial Data Set** means an identifiable collection of spatial data which –

(a) Are in an electronic format
(b) Relate to one or more of the themes listed in Annex I, II or III to the Directive, and
(c) Relate to –
    (i) The United Kingdom
    (ii) Gibraltar
    (iii) The territorial sea of the United Kingdom
    (iv) The area of the continental shelf for the time being designated by an Order in Council under section 17(1) of the Continental Shelf Act 1964, or
    (v) An area, outside the territorial sea of the United Kingdom, for the time being designated by an Order in Council under section 84(4) of the Energy Act 2004.

**Spatial Data Services** means a service which consists of operations which may be performed, by invoking a computer application –

(a) On the spatial data contained in a spatial data set, or
(b) On the metadata related to a spatial data set.

**Subject Access Request** – the right given by the Data Protection Act 1998, to an individual to ask the Council for a copy of the personal data being processed by the Council. However, there are exemptions that may be applied in certain circumstances and copies of all the personal data will be provided in response to every request. The information must be supplied in an intelligible form and in a permanent form unless this would involve disproportionate effort or if the individual agrees otherwise. The Council may have to consider the Disability Discrimination Act requirements when providing personal data to an individual who may require the information to be provided in a certain format to take a special need into account.

**T**

**U**

**V**

**Vital records:** are records classified as being essential to the continuation of Council business.

**W**

**Working day** means any day other than a Saturday, Sunday, Christmas Day, or a Day which, under the Banking and Financial Dealings Act 1971 is a bank holiday in Scotland.

**X**

**Y**

**Z**

# Appendix 2B; Information Council Responsibilities

1. Provide strategic leadership for information governance and information risk management throughout the Council.

2. Support and monitor the development of the Information Governance Framework and its implementation, including all accompanying policies, guidance and tools.

3. Agree, support and monitor the annual information governance plan to drive change, including plan revision and realignment to mitigate risk.

4. Take ownership of the information risk management approach, including monitoring compliance with the Information Governance Framework, reporting and escalating information risks as appropriate, taking corrective actions where necessary, and maintaining the corporate risk register.

5. Receive and consider reports into breaches of confidentiality and security and, where appropriate, undertake or recommend remedial action.

6. Develop solutions and implementation programmes (including training and raising awareness) to ensure that the Council complies with developing information governance requirements.

7. Ensure that each Directorate and service fulfil their responsibilities and apply relevant information governance policies and controls.

8. Support managers with the implementation of information governance standards and policies, the management of information risks, and in promoting awareness throughout their service areas.

9. Support audit and assessment arrangements for information governance (internal and external).

10. Undertake an annual maturity assessment to measure progress and improvement.

11. Ensure the Council Management Team and Elected Members are appropriately and regularly briefed on information governance and risk issues.

12. Ensure that Council's approach to information governance and information risk is effective in terms of resource, commitment and execution, and that it is communicated to all service areas and staff.

13. Create, direct and support subsidiary groups (e.g. Data Council) in developing, maintaining and complying with the Information Governance Framework.

14. Liaise with other working groups and programme boards to ensure compliance with the Council's Information Governance Framework.

15. Provide a focal point for the resolution and/or discussion of information governance and risk issues.

# Appendix 3 - Data Protection Policy

## Policy statement

1.1. This policy sets out and formalises the City of Edinburgh Council's (the Council) approach for ensuring that personal information is properly processed, managed and protected in accordance with the requirements of the Data Protection Act 1998.All personal data held, maintained and used by the Council in all locations and in all media (paper and electronic).

1.2. It outlines the Council's commitment to the principles enshrined within the Act, and the need to balance the rights of individuals with the functions and operational requirements of the Council.

## Scope

2.1. This policy applies to:

2.1.1 All personal data held, maintained and used by the Council in all locations and in all media (paper and electronic).

2.1.2 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 personal data on the Council's behalf when carrying out a statutory Council function or service.

## Definitions

3.1 The definitions below cover specific terms and descriptions used in this policy.

3.2 **Criminal Offences under the Data Protection Act 1998** – In Scotland criminal proceedings for an offence under the Data Protection Act 1998 will be brought only by the Procurator Fiscal. In England, Wales and Northern Ireland proceedings can be commenced by the Information Commissioner. The offences under the Data Protection Act 1998 are:

3.2.1 Processing without a valid Notification;

3.2.2 Failure to advise the Information Commissioner of changes to the Notification;

3.2.3 Failure to comply with an Information Notice;

3.2.4 Failure to comply with an Enforcement Notice;

3.2.5 Unlawfully obtaining or disclosing personal data;

3.2.6 Procuring the disclosure of personal data; and

3.2.7 Unlawfully selling personal data;

3.2.8 Enforced subject access.

3.3 **Data controller –** a legal person or organisation who determines the purposes for which, and the 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 purpose of constituency work.

3.4 **Data processor –** is a person, other than an employee of the Council, who processes personal data on behalf of the Council. This processing must be evidenced in a written contract. The data processor can only use personal data under the instructions of the Council. The Council retains full responsibility for the actions of the data processor in relation to the personal data.

3.5 **Data Protection Act 1998** – gives effect in the UK law to the EC Directive 95/46/EC and came into force on 1 March 2000 repealing the Data Protection Act 1984. The Data Protection Act 1998, together with a number of Statutory Instruments, requires data controllers to comply with the legislation governing how personal data is used for statutory and business purposes. Amendments have also been created by other legislation such as the Freedom of Information Act 2000. It gives rights to individuals in relation to how organisation can use their personal data.

3.6 **Data subject** – a living individual who can be identified from the personal data or from additional information held, or obtained, by the Council. For example, a CCTV image which can identify someone when linked to building access control codes.

3.7 **Enforcement Notice** – The Information Commissioner has the power to serve an enforcement notice on a data controller if he determines that a data controller has failed to comply with the requirements of the Data Protection Act 1998. The Notice sets out the actions that the data controller must take to achieve compliance. A data controller can lodge an appeal against the Notice to the Information Tribunal. If the data controller fails to comply with a valid Enforcement Notice this is a criminal offence under the Data Protection Act 1998.

3.8 **Information Commissioner** – is responsible for the regulation of the Data Protection Act 1998 throughout the UK. The Information Commissioner is appointed by the Queen and is independent of the UK Government.

3.9 **Information Notice** – an Information Notice can be issued by the Information Commissioner which requires a data controller to provide his office with information that he requires to carry out his functions. Failure to comply with an Information Notice is a criminal offence.

3.10 **Information security** – ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

3.11 **Information sharing** – ensures that the Council information is shared in a compliant, controlled and transparent manner.

3.12 **Mandate** - provides authorisation for the release of personal data in line with the provisions of the Data Protection Act 1998.

3.13 **Notification** - the Council is required to notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. Failure to Notify is a **criminal offence**. The Council must inform the Information Commissioner of any changes to the processing of personal data and renew the Notification annually. Failure to do so is also a **criminal offence**. The Information Commissioner maintains, and publishes, a Register of Data Controllers.

3.14 **Elected Members** are required to lodge, and maintain, a separate Notification to cover constituency work. Failure to do so is a **criminal offence.**

3.15 **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.

3.16 **Privacy 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 changes to service activities, or new ICT impact on the privacy of individuals.

3.17 **Processing** – is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

3.18 **Sensitive Personal Data** – requires a higher level of consideration. The following categories are defined as 'sensitive personal data' for the purposes of the Data Protection Act 1998 –

3.18.1 Racial or ethnic origin of the data subject;

3.18.2 Political Opinions;

3.18.3 Religious or similar beliefs;

3.18.4 Trade Union membership;

3.18.5 Physical or mental health or condition;

3.18.6 Sexual life; and

3.18.7 Criminal offences or alleged criminal activity (and any criminal proceedings).

3.19 **Subject Access Request** – the right given by the Data Protection Act 1998, to an individual to ask the Council for a copy of the personal data being processed by the Council. However, there are exemptions that may be applied in certain circumstances and copies of all the personal data will be provided in response to every request. The information must be supplied in an intelligible form and in a permanent form unless this would involve disproportionate effort or if the individual agrees otherwise. The Council may have to consider the requirements under the Equalities Act 2010 when providing personal data to an individual who may require the information to be provided in a certain format to take a special need into account.

3.20 The **European Economic Area** provides for the free movement of goods and persons through member states of the European Union and three of the member states of the European Free Trade Association (Iceland, Liechtenstein and Norway)

# Policy content

### Introduction

4.1 The Council needs to collect and use information about its customers to facilitate the effective delivery of services. The Data Protection Act 1998 ensures that this information is gathered, used, stored, shared, protected, retained and destroyed in a way which is fair and lawful.

### Data Protection Principles

4.2 The basis of the Act is set out in the eight data protection principles which the Council must comply with in relation to personal information.

4.3 **Data Protection Principle 1** - Personal data shall be processed fairly and lawfully

4.3.1 The Council regularly collects personal data from individuals who receive services or have a relationship with the Council (e.g. suppliers, employees). In accordance with the conditions set out in the Data Protection Act 1998, the Council will ensure that there is a fair and lawful basis for collecting and processing personal data.

4.4 **Data Protection Principle 2** – Personal data shall be obtained for one or more lawful purposes, and not processed in a manner incompatible with that purpose.

4.4.1 The Council will explain why it is collecting personal data and how it intends to use that data. A regular review of personal information gathering forms and methods will be undertaken by the Information Governance Unit to ensure legal compliance, taking into account the *Code of Practice on Privacy Notices* produced by the Information Commissioner.

4.4.2 To provide customers with a better service and to fulfil the Council's statutory functions, personal data collected across Council services may be used in different ways, if its use is deemed appropriate and fair. Individuals will be advised if their personal data is to be used in a new way.

4.4.3 Privacy impact assessments must be carried out by service areas when:

4.4.3.1 Council projects or programmes are undertaken;

4.4.3.2 Service activities commence, end or are significantly adjusted; and/or

4.4.3.3 New ICT arrangements are put in place which use and process personal data with a potential impact on the privacy of individuals.

4.5 **Data Protection Principle 3** – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.5.1 The Council will only obtain, use and retain personal information that it actually needs to fulfil its business and operational requirements.

4.6 **Data Protection Principle 4** – Personal data shall be accurate and, where necessary, kept up to date.

4.6.1 The Council must ensure that personal data is accurate, relevant and current to facilitate the effective delivery of services. Individuals have a right to compensation if damage has been caused to them by the Council taking decisions about them based on out of date and/or inaccurate information.

4.7 **Data Protection Principle 5** – Personal data processed for any other purpose or purposes shall not be kept for any longer than is necessary for that purpose or purposes.

4.7.1 Personal data must be retained and disposed off in accordance with the Council's Record Retention and Disposal Schedules. Retention rules apply to both hardcopy and electronic formats.

4.7.2 All personal data must be disposed off securely and appropriately.

4.8 **Data Protection Principle 6 -** Personal data shall be processed in accordance with the rights of data subjects (including a right of Subject Access).

4.8.1 Requests for personal information (subject access requests):

4.8.1.1 Section 7 of the Data Protection Act 1998 gives individuals the right to ask what personal information is held about them, and to obtain a copy of that information, subject to limited exemptions.

4.8.1.2 Subject access requests are logged and processed by the Information Governance Unit and must be responded to within 40 calendar days. The Unit will ask individuals to provide proof of identity to verify requests, or ask for authorisation to disclose if a request is being made on behalf of an individual.

4.8.1.3 If an individual believes the Council has not complied with the Data Protection Act 1998, they can refer their concerns to the Information Commissioner's Office and ask them to undertake an assessment of how the Council has dealt with their request.

4.8.1.4 The Data Protection Act 1998 gives data controllers the right to charge a fee of £10.00 (the fee can be higher for different types of records, such as school records). The Council does not routinely charge for subject access requests, but reserves the right to do so.

4.8.2 Prevention of processing causing damage or distress

4.8.2.1 Individuals can ask the Council, in writing, to stop using their personal data if they consider that the processing of their data is causing them substantial unwarranted damage or distress. The individual is not entitled to serve such a notice if any of the following conditions for using their personal information apply:

4.8.2.2 the individual has given a valid consent to the use of their personal information;

4.8.2.3 the use of the personal information is required for the purpose of a contract with the individual;

4.8.2.4 the use of the personal information is necessary for any legal obligation placed on the Council;

4.8.2.5 the use of the personal information is necessary to protect the vital interest of the individual.

4.8.2.6 The Council must respond within 21 calendar days if a notice to cease using personal information is received.

4.8.3 Right to rectification, blocking, erasure and destruction of personal data

4.8.3.1 An individual has the right to have any inaccurate personal data corrected, blocked, erased or destroyed in circumstances where the personal data is inaccurate (as a matter of fact).

4.8.3.2 If individuals disagree with a professional opinion which has been recorded about them, a note will be added to their record.

4.8.4 Rights in relation to automated decision making

4.8.4.1 An individual is entitled to ask the Council, in writing, that any decision which has a significant effect on them is not based solely on automated decision making methods.

4.8.5 Rights to compensation

An individual who suffers damage or distress as the result of contravention of the Act by the Council may seek compensation by application to the Court.

4.9 **Data Protection Principle 7** – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to, personal data.

4.9.1 Information security

4.9.1.1 Personal data must be kept secure at all times. The Council's Guidance Note on Protecting Personal Data and the ICT Acceptable Use Policy provide practical advice that must be followed to protect personal data in the possession of the Council.

4.9.2 Data breaches

4.9.2.1 Data breaches can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, files containing personal data). It can also occur through the unauthorised use or

accidental disclosure of personal data by employees, and deliberate attacks on Council systems.

4.9.2.2 All breaches involving personal and sensitive personal data must be reported to the Information Governance Unit, in line with the Council's Data Breach Procedure. This will allow the Council to take all the necessary steps to recover the data and limit any potential damage caused by the breach.

4.10 **Data Protection Principle 8** – Personal information must not be transferred to countries outside the European Economic Area unless that country has adequate protection for the rights and freedom of individuals in respect of the use of personal information

4.10.1 While the Council does not routinely transfer personal information outside the United Kingdom and the European Economic Area, there may be occasions when this required. The Information Governance Unit will advise and ensure that there are appropriate safeguards in place to satisfy the 8th principle.

**Disclosure**

4.11. **Disclosure of personal information**

4.11.1 There are many instances where personal data can be disclosed with (and without) the consent of the individual. For example, information may be shared with other agencies through partnership arrangements – a process governed by data sharing agreements. Individuals may also authorise disclosure through a mandate. On such occasions, only the personal data that is necessary should be disclosed. When considering the disclosure of information attention must be given to protective marking scheme categories.

4.12 **Disclosure of personal data to Elected Members**

4.12.1 Elected members may request personal data in the course of their work, for example as a committee member, or acting on behalf of a constituent. Elected Members will be given access to the personal data they need to carry out their duties, in line with the Member/Officer Protocol.

4.13 **Disclosure of personal data relating to crime and taxation**

4.13.1 Section 29 of the Data Protection Act 1998 allows the Council to consider disclosing personal data for the purpose of prevention or detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of taxes or duties. Each request is considered on a case by case basis and must be forwarded to the Information Governance Unit for processing and response.

4.14 **Disclosure of data required by law**

4.14.1 Section 35 of the Data Protection Act 1998 allows the Council to consider releasing information in relation to legal proceedings. Each request is

considered on a case by case basis and must be forwarded to Information Compliance for processing and response.

4.15 **Business as usual requests**

4.15.1 If an individual requests personal data that has already been sent or disclosed to that individual (for example, a letter that has been sent previously), then service areas should treat such requests as business as usual requests and send replacement copies, subject to confirming proof of identity.

**4.16 Unauthorised disclosure**

4.16.1 Employees (and others covered by this policy) must never disclose personal data obtained in the course of their work with the Council, or access personal data without appropriate permissions. It is a criminal offence under section 55 of the Data Protection Act 1998 to knowingly obtain or disclose personal data without the consent of the data controller (the City of Edinburgh Council).

**Data sharing**

4.17 The Council works with other public agencies to provide services. The sharing of personal data between the Council and other public authorities is subject to formal data sharing protocols which set out overarching common rules adopted by the Council and other public agencies with whom it wishes to share data. Details of each data sharing process are documented in data sharing agreements. A central register of all protocols and agreements will be maintained by the Information Governance Unit to ensure that transfer and sharing arrangements meet the requirements of the Data Protection Act 1998, and the Information Commissioner's Code of Practice on Data Sharing. All new data sharing protocols and agreements must be assured by the Information Governance Unit in the first instance.

**Data processing**

4.18 Contractors and consultants will carry out work and process personal data on the Council's behalf to help deliver services. In such cases, the Council is considered to be the 'data controller' responsible for that personal data, and the contractor or consultant as the 'data processor' who processes that data on behalf of the Council. Such arrangements must be governed by written agreements or contracts to ensure compliance with this policy and the data protection principles, including on-going monitoring. Legal Services must be consulted before engaging contractors or consultants who process personal data.

**Notification**

4.19 As a Data Controller, the Council has to notify the Information Commissioner about the types of personal data it collects and processes. The Council's notification is included on the Data Protection Register which is available on the Commissioner's website. The Information Governance Unit is responsible for compiling and renewing the Council's notification each year. It is a criminal offence not to notify the Information Commissioner, if there is a requirement to do so. Failure to maintain an up to date notification, if required to do so, is a criminal offence.

### Information Asset Register

4.20 An Information Asset Register will be maintained by the Information Governance Unit. The register identifies personal data and sensitive personal data held by the Council, and helps to evaluate and assure compliance with the Council's information governance policies and processes, recording and highlighting risk as appropriate.

### Training

4.21 All employees, contractors, consultants and volunteers need to be aware of their obligations under the Data Protection Act 1998. A variety of training methods will be employed to ensure appropriate levels of awareness, understanding and knowledge.

## Implementation

5.1 The Information Council will approve and monitor an annual action plan for information governance development and compliance, including data protection. The plan will outline key tasks, outcomes, accountabilities and progress.

## Roles and responsibilities

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to compliance with the Data Protection Act 1998.

### Elected Members

6.2 Elected members are covered by the Council's notification when carrying out official duties for the Council but they are required, by law, to hold a separate notification for constituency work. Elected member notification is administered by the Information Governance Unit.

### Corporate Management Team

6.3 The Corporate Management Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate applies relevant information governance policies and controls, including compliance with the requirements of the Data Protection Act 1998. Responsibility also extends to personal data that is processed by third parties within their respective areas of responsibility.

### Senior Information Risk Owner

6.4 The Director of Corporate Governance is the Council's Senior Information Risk Owner (SIRO).The SIRO has delegated authority through the Corporate Management Team with specific responsibility for information risk and mitigation, ensuring that any information threats and breaches are identified, assessed and effectively managed.

### Governance Manager

6.5 The Governance Manager is the Deputy Senior Information Risk Owner and deputises for the SIRO as required.

### Information Council

6.6 The Information Council (IC) has delegated responsibility, through the SIRO and the Corporate Management Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure compliance with the Data Protection Act 1998. The IC is chaired by the Deputy SIRO.

### Information Governance Unit

6.7 The Information Governance Unit is part of the Governance Service with responsibility for the day to day operation and delivery of information governance within the Council. In relation to data protection it will:

6.7.1 Act as the first point of contact for all data protection issues affecting the Council;

6.7.2 Provide guidance and advice on data protection issues for all Council directorates;

6.7.3 Renew and amend the Council's data protection notification to the ICO, as advised by managers;

6.7.4 Co-ordinate, process and respond to all subject access requests;

6.7.5 Oversee and quality assure all data sharing protocols and agreements between the Council and other partner agencies;

6.7.6 Record and maintain the Council's information risk register, including risks relating to data protection and associated information governance activities;

6.7.7 Create, maintain and renew training modules and toolkits as appropriate;

6.7.8 Provide data protection training and awareness raising (as requested);

6.7.9 Maintain and report on key performance indicators for information governance;

6.7.10 Lead and advise on compliance requirements where the processing of personal information is complex (e.g. multi-agency working);

6.7.11 Co-ordinate the Council's information breach procedures; and

6.7.12 Carry out information governance assessments.

**Managers**

6.8 All managers must:

6.8.1 Ensure that this policy and any associated procedures governing the use of personal information (corporate and local) are in place, understood and followed by all staff within their business areas;

6.8.2 Ensure that their staff have received data protection training (appropriate to their role), and maintain records as to when initial and refresher training has taken place;

6.8.3 Review and revise procedures if processes governing the use of personal information are subject to change within their business areas;

6.8.4 Consult the Information Governance Unit when there is a proposed change to the use of personal information, or when new projects are being considered;

6.8.5 Undertake Privacy Impact Assessments in respect of new projects or new processing of personal information;

6.8.6 Consult the Information Governance Unit before signing up to, or revising, any information sharing protocol or agreement;

6.8.7 Report any suspected breaches of confidentiality or information loss to the Information Governance Unit and follow the breach reporting procedure;

6.8.8 Identify any existing or emerging information risks relating to personal information and report to the Information Governance Unit and, if required, record on local, divisional and directorate risk registers;

6.8.9 Ensure that personal data required to answer a subject access request is provided timeously to the Information Governance Unit;

6.8.10 Ensure that there are appropriate procedures and measures in place protect personal data, particularly when that information (hardcopy and electronic) is removed from Council premises;

6.8.11 Undertake annual information governance self-assessments to ensure on-going compliance with this policy and associated information governance activities;

6.8.12 Provide a statement of assurance to evidence information governance compliance; and

6.8.13 Inform the Information Governance Unit (when requested) of activities containing personal data (paper or electronic) to facilitate the Council's notification process with the Information Commissioner.

**Employees**

6.9 All employees have a responsibility for data protection and must:

6.9.1 Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their work;

6.9.2 Undertake data protection training (including annual refresher training) and ensure they have a clear understanding of their responsibilities in using and handling personal information;

6.9.3 Identify and report any risks to personal information to their line manager

6.9.4 Identify and report suspected breaches of confidentiality or compromised personal data to their line manager;

6.9.5 Identify and forward any subject access requests to the Information Governance Unit to ensure that requests can be processed in accordance with the statutory timescales; and

6.9.6 Assist customers in understanding their information rights and the Council's responsibilities in relation to data protection.

# Related documents

7.1 Related documents include:

7.1.1 Information Governance Strategy

7.1.2 Information Governance Policy

7.1.3 Records Management Policy

7.1.4 Freedom of Information Policy

7.1.5 Data Quality Policy

7.1.6 ICT Acceptable Use Policy

7.1.7 Employee Code of Conduct

7.1.8 Open Data Strategy

# Equalities impact

8.1 There is no adverse impact on any group in terms of race, religion, disability, ethnic origin, sexuality or age in relation to this policy.

The Act includes clauses relating to information about young children and secondary legislation provides legislative grounds to be followed when dealing with personal information about people who have a limited capacity as to the understanding of their rights under the Act. Secondary legislation also provides clauses to ensure compliance with specific categories of information such as adoption and education records.

# Sustainability impact

9.1 There are no sustainability issues arising from this policy.

# Risk assessment

10.1 Failure to comply with any requirement of the Act could result in enforcement action by the ICO. The ICO has powers to impose a Civil Monetary Penalty which can result in a fine of up to £500 000 for each breach. This amount could rise considerably subject to the adoption of the Data Protection Regulation under consideration by the European Parliament.

10.2 Individuals may take action against the Council through the Court for any misuse of their personal information. Depending on which Court takes the action fines could be unlimited.

10.3 Failure to renew or amend the Council's Data Protection Notification as required by the Act will result in a criminal offence.

10.4 Failure to respond to any of the time critical response requirements in relation to information rights for individuals will result in a breach of the Act.

10.5 Mishandling of personal information will have a serious reputational impact to the Council.

10.6 Mishandling of personal information may have serious implications to one, or more, individuals.

10.7 Personal information that is inaccurate or out of date may result in a serious negative impact on one or more individuals.

# Review

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

# Appendix 4 - Data Quality Policy

## Policy statement

1.1 The City of Edinburgh Council (the Council) needs reliable, relevant, accurate and timely data to help deliver services and to account for its performance. Data quality is a key element of the Council's Information Governance Strategy and this policy sets out the Council's commitment and approach to improving its creation, management and use.

## Scope

2.1 This policy relates to:

2.1.1 All Council data and information collection activities.

2.1.2 Council staff, including temporary staff, contactors and consultants that create, use and manage data.

2.1.3 All third parties that create, process and use data on the Council's behalf when carrying out a statutory function or service.

## Definitions

3.1 The definitions below cover specific terms and descriptions used in this policy.

3.2 **Data:** the raw input from which information of value is derived.

3.3 **Data quality:** recognition that the accuracy, coverage, timeliness and completeness of data can significantly impact on the value of its use.

3.4 **Data stewards** are nominated by Information Asset Owners with operational responsibility for information assets within their respective service areas. This will involve the application of information governance rules, and the up-dating of Council data and records to help ensure data integrity and quality.

3.5 **Information asset:** a body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

3.6 **Information asset owners:** senior officers involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

3.7 **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.

# Policy content

4.1 Data quality is concerned with producing information that is 'fit for purpose' and available when required. It supports service provision and the Council's business operations by ensuring that any data collected, used, recorded and shared is accurate, complete and reliable.

4.2 It also ensures that Council decisions are based on reliable management and performance information, and provides confidence when benchmarking or producing reports and statistical analysis for internal and external audiences.

4.3 The production and availability of high quality data also supports the Council's objectives to be open and transparent, and aligns closely with the Council's open data strategy.

4.4 Quality data also helps the Council comply with its obligations under the Data Protection Act 1998.

4.5 To assure the quality of data, the Council will adopt the following principles which will be supported procedures, guidance and training.

Data collection

4.5.1 **Accuracy**: Data must be accurate with clear procedural guidance for collecting, using and amending data.

4.5.2 **Timeliness:** Data should be collected as quickly as possible after the event or activity, and must be available quickly enough to support information/ business needs and management decisions

4.5.3 **Relevance:** Data must be relevant to the purposes for which it is used, and must be reviewed on a regular basis to reflect changing needs, including changed service or legislative requirements.

Data management

4.5.4 **Reliability:** Data collection processes must be clearly defined and followed to ensure on-going stability and consistency over time. In particular, trend data must reflect real change rather than variations in data collections methods or approaches.

4.5.4 **Verification:** Data must be verified on a regular basis to ensure that there are no gaps, and that systems do not contain redundant or duplicate records. Verification approaches include:

4.5.4.1 Data cleansing to remove duplicate records or complete missing information

4.5.4.2 Signing-off processes to verify that data has been checked

4.5.4.3 Regular query reports to check system integrity

4.5.4.4 Regular checks and sampling to quality assure data accuracy

Data presentation

4.6 **Validity**: Data needs to be presented in line with relevant requirements, rules and definitions to ensure clarity, consistency and comparability, in particular performance and open data.

# Implementation

5.1 The Information Council will approve and monitor an annual action plan for information governance development and compliance, including data quality. The plan will detail key tasks, outcomes, accountabilities and progress to ensure high standards of data quality, based on the principles listed above.

# Roles and responsibilities

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to using, managing and improving the quality of the Council's data.

### Corporate Management Team

6.2 The Corporate Management Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate applies relevant information governance policies and controls, including compliance with this policy. In particular, directors will be asked to nominate/ confirm information asset owners and data stewards.

### Senior Information Risk Owner

6.3 The Director of Corporate Governance is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Corporate Management Team with specific responsibility for information risk and mitigation, including risks around the quality of the Council's data. The Governance Manager is the Deputy Senior Information Risk Owner and deputises for the SIRO as required.

### Information Council

6.4 The Information Council (IC) has delegated responsibility, through the SIRO and the Corporate Management Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure compliance with this policy.

**Data Council**

6.5 The Data Council has delegated authority through the IC and supports the implementation of the information governance strategy particularly the Data Quality work stream. The Data Council is chaired by the Information Governance Manager. Key responsibilities include:

6.5.1 Supporting and improving data quality in the Council

6.5.2 Supporting the development of guidance and training around data quality

6.5.3 Providing information and guidance on data management processes

**Information Governance Unit**

6.6 The Information Governance Unit will support the implementation of this policy as set out in the IC annual plan.

**Managers and supervisors**

6.7 All managers must:

6.7.1 Ensure that clearly documented systems and processes are in place to deliver high quality data

6.7.2 Ensure arrangements in place to quality assure data, and carry out on a regular basis

6.7.3 Ensure staff have the necessary skills and knowledge required to capture, process and deliver high quality data

6.7.4 Never knowingly use inaccurate or incomplete data for reporting purposes, and highlight any known risks or issues to the Information Asset Owner

6.8 As the Information Asset Register is developed and extended to identify and manage the Council's information assets, relevant managers will be designated as Information Asset Owners, including responsibilities for data quality

**Staff**

6.9 All staff must:

6.9.1 Read, understand and follow this policy and any associated procedures that relate to the capture, use and management of Council data

6.9.2 Handle Council data in a way which is responsible and make every effort to ensure its accuracy, validity, reliability, timeliness, relevance and verifiability

6.9.3 Communicate any risks or concerns to line managers concerning the capture or use of data

6.10 As part of their role and remit, individuals may also be nominated as Data Stewards (by Information Asset Owners) with operational responsibility for data quality issues.

# Related documents

7.1 Related documents include:

7.1.1 Information Governance Strategy
7.1.2 Information Governance Policy
7.1.3 Records Management Policy
7.1.4 Freedom of Information Policy
7.1.5 Data Quality Policy
7.1.6 ICT Acceptable Use Policy
7.1.7 Employee Code of Conduct
7.1.8 Open Data Strategy

# Equalities impact

8.1 There are no equalities issues arising from this policy.

# Sustainability impact

9.1 There are no sustainability issues arising from this policy.

# Risk assessment

10.1 The risks of not implementing this policy include:

10.1.1 Ineffective and poor decision making
10.1.2 Lack of accountability and reliable performance information
10.1.3 Inefficient service delivery
10.1.4 Financial loss or monetary penalty imposed
10.1.5 Detrimental impact on Council business and service delivery
10.1.6 Non-compliance with legislation and potential litigation

# Review

11.1 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 Council and presented to Council committee annually, in line with the Council's Policy Framework.

# Appendix 5- Freedom of Information Policy

## Policy statement

1.1 This Policy formalises the City of Edinburgh Council's approach to the management and release of information and sets out the Council's commitment to the following principles:

1.1.1 To conduct its business in such a way as to promote openness and accountability thereby maximising public trust in the workings of the Council

1.1.2 To take into account customer needs in presenting information

1.1.3 To maximise the publication of information through the Council's publication scheme

1.1.4 To respect personal privacy in accordance with the principles set out in the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, and the Data Protection Act 1998.

## Scope

2.1 This policy applies to the rights of any person, anywhere in the world to request access to recorded information held by the Council, subject to certain limited conditions and exemptions, exceptions or limitations.

2.2 The policy is applicable to all recorded information, of any age and in any format, held by the Council within the definition contained in the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. It is also applicable to all spatial data sets, or spatial data services about the environment or meta data relating to these as defined by the INSPIRE (Scotland) Regulations 2009.

2.3 This policy applies to all employees of the Council and elected members when carrying out official duties for the Council. It also applies to third parties who hold or manage information on the Council's behalf.

2.4 Any contractor or agent performing work for, or on behalf of the Council, will be required to assist the Council in implementing its obligations under the Act and Regulations, with particular reference to the prompt provision of information where requested by the Council.

# Definitions

3.1 The definitions below concern specific terms and descriptions used in this policy.

3.1.1 **Exception:** This is a regulation under regulations 10 or 11 of the Environmental Information (Scotland) Regulations 2004 which, if applicable to information covered by the request, means that the information does not need to be disclosed.

3.1.2 **Exemption:** This is a section in Part 2 of the Freedom of Information (Scotland) Act 2002 which, if applicable to information covered by the request, means that the information does not need to be disclosed.

3.1.3 **Information:** This is information recorded in any form or format held by the Council, or information held by a third party on the Council's behalf.

3.1.4 **Limitation:** This is a regulation under regulation 10 of the INSPIRE (Scotland) Regulations 2009 which, if applicable to the information covered by the request, means that the information does not need to be disclosed.

3.1.5 **Personal data:** This 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.

3.1.6 **Records management:** These are the 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. International Standard **ISO15489** covers the fundamentals of good records management.

3.1.7 **Scottish Information Commissioner:** is responsible for the promotion and enforcement of the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009 and any associated Codes of Practice.

# Policy content

### Legislation

4.1 The Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 provide any person, anywhere in the world, with a general right of access to recorded information held by the Council. This is subject to certain limited conditions and exemptions/exceptions.

4.2 The legislation also places certain duties on the Council regarding the management of its records. The Council is also required to prepare and

maintain a Publication Scheme, setting out the information that it routinely makes available, and which can be accessed quickly and easily.

4.3 The INSPIRE (Scotland) Regulations 2009 provide any person, anywhere in the world, with a right of access to any spatial datasets or spatial data services about the environment together with the meta data related to these, subject to certain conditions and limitations.

4.4 The Scottish Ministers have published two Codes of Practice under the Freedom of Information (Scotland) Act 2002. These provide best practice guidance to public authorities on discharging their function under the Freedom of Information (Scotland) Act 2002 as follows:-

4.4.1 Section 61 Code of Practice on Records Management; and

4.4.2 A combined Section 60 and 62 Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 and the Environmental (Scotland) Regulations 2004.

**Rights to information**

4.5 A request for recorded information held by the Council can be made by any person.

4.6 A request for information may be covered by one or more of three information rights:

4.6.1 A request for recorded information held by the Council, other than for the requestors own personal data or for environmental information, is a Freedom of Information request.

4.6.2 A request for any recorded information which relates to matters such as air, water, soil, landscaping, natural sites, biodiversity, human health and safety and decisions and activities affecting these is a request covered by the Environmental Information (Scotland) Regulations 2004.

4.6.3 A request for spatial datasets or spatial data service about the environment or the meta data related to these which is held by the Council is a request covered by the INSPIRE (Scotland) Regulations 2009.

4.7 The Council will ensure that any information that has been requested will be made available, unless there is a compelling reason and basis in law for withholding it.

**Publication scheme**

4.8 In line with the requirements of the Freedom of Information (Scotland) Act 2002 the Council has a publication scheme which is available on the website. This is a guide to the information that the Council routinely makes publicly available.

**Open Data Initiative**

4.9 The Council will, where possible, identify data which is already readily available and which can be shared publicly.

**Dealing with requests**

4.10 The Council will respond to all requests promptly, and within the statutory response period of 20 working days following receipt of a valid request.

4.11 Under the Environmental Information (Scotland) Regulations the Council can extend the timescale for responding to a request in certain circumstances. The requestor will be notified if the Council does intend to extend the timescale for response and the reason why.

4.12 The Freedom of Information (Scotland) Act 2002 provides a number of exemptions which can be relied upon to withhold information. The Environmental Information (Scotland) Regulations provides a number of exceptions which can be relied upon to withhold information, and under the INSPIRE (Scotland) Regulations limitations can be used to withhold information.

4.13 Where the Council is seeking to rely on any exemption, exception or limitation for withholding information from a requestor, it will explain, in detail, why this applies to the information requested.

**Redaction**

4.14 The Council will not routinely redact the names of Council officials from information produced in the course of their work, but will take into account specific circumstances, and the latest guidance from Information Commissioner's Office and the Office of the Scottish Information Commissioner.

**Charges**

4.15 There is generally no charge for information provided in the Council's Publication Scheme, unless otherwise stated and in some cases there is a charge for printing and postage.

4.16 As far as other requests are concerned, the Council is not entitled to charge for requests that cost less than £100 to process. The Council will charge 10% of the cost of dealing with requests costing between £100 and £600 respectively. These charges are based on the:

4.16.1 Estimated costs of staff time to find information;
4.16.2 Any costs associated with putting information into a particular format; and
4.16.3 Copying and postage costs.

4.17 The Council cannot, and does not, charge for the time taken to decide whether it holds relevant, recorded information, or whether it can be disclosed.

4.18 Different charges apply under the Environmental Information (Scotland) Regulations 2004.

4.19 Unlike the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 do not specify an upper or limit when fees can be charged. The Environmental Information (Scotland) Regulations prescribe that any fee charged must not exceed the actual costs to the Council of producing the information requested. The Council can only charge fees under the Regulations in line with its published charging schedule. In assessing what cost to charge, the Council considers the matters covered above regarding Freedom of Information (Scotland) Act 2002 requests.

4.20 Under the INSPIRE (Scotland) Regulations the Council can only charge the public to view information where that charge secures the maintenance of spatial data sets and spatial data services, especially in cases which involve very large volumes of frequently updated data.

4.21 The Council may charge the public a reasonable sum for downloading services, enabling copies of spatial data sets, or parts of such sets to be downloaded and, where practicable, accessed directly.

4.22 The Council may charge the public a reasonable sum for transformation services, enabling spatial data to be transformed with a view to achieving interoperability and also services which allow spatial data services to be invoked.

4.23 Charges levied by the Council under the INSPIRE (Scotland) Regulations 2009 are required to be kept to the minimum required and will be in line with existing Council charging policies.

**Disclosure Log**

4.24 The Council has a publicly available disclosure log which records all requests for information received. This also shows the responses issued in relation to those requests.

**Requirements for Review**

4.25 Where an applicant is dissatisfied with the response to their information request, they are entitled to seek a review of the Council's decision. A response to their requirement for review will be provided within 20 working days.

**Appeal**

4.26 If the applicant remains dissatisfied following the outcome of their requirement for review, they are entitled to appeal to the Scottish Information Commissioner, who will investigate the Council's handling of their information request.

**Records Management**

4.27 Information is an extremely valuable resource and must be looked after properly. In managing its records, the Council will comply with its duties under the Freedom of Information (Scotland) Act 2002 and the Section 61 Code of Practice on Records Management.

### Compliance

4.28 All recorded information will be managed in accordance with the Freedom of Information (Scotland) Act 2002 and the associated Codes of Practice.

### Monitoring and reporting

4.29 Compliance with this policy and related procedures will be monitored by the Information Governance Manager.

4.30 Performance reports will be submitted to Elected Members and Corporate Management Team on a regular basis.

## Implementation

5.1 This policy will be implemented as part of the Information Council's annual action plan.

## Roles and responsibilities

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to compliance with the Freedom of Information (Scotland) Act 2002 and associated legislation.

### Elected Members

6.2 All Elected Members will be provided information and training on the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009.

### Corporate Management Team

6.3 The Corporate Management Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate applies relevant information governance policies and controls, including compliance with the requirements of the Freedom of Information (Scotland) Act 2002 and associated legislation.

**Senior Information Risk Owner**

6.4 The Director of Corporate Governance is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Corporate Management Team with specific responsibility for information risk and mitigation, ensuring that any information threats and breaches are identified, assessed and effectively managed.

**Governance Manager**

6.5 The Governance Manager is the Deputy Senior Information Risk Owner and deputises for the SIRO as required.

**Information Council**

6.6 The Information Council (IC) has delegated responsibility, through the SIRO and the Corporate Management Team, for the development and delivery of effective information governance throughout the Council. In particular, the IC will provide the necessary ownership and advocacy required to support, co-ordinate, promote, monitor and assure compliance with the Freedom of Information (Scotland) Act 2002 and associated legislation.

**Information Governance Unit**

6.7 The Information Governance Unit will:

6.7.1 Act as the first point of contact for all freedom of information issues affecting the Council;

6.7.2 Log, process and respond to all information requests received by the Council;

6.7.3 Assess and log requests and allocate to the relevant service to ask them to identify any relevant, recorded information that they hold which would fulfil the request;

6.7.4 Provide the final decision as to whether any exemption/exception/limitation applies to the information requested from the Council; and

6.7.5 Publish details of all requests and the responses to these on the Council's disclosure log.

**Freedom of Information Team Leader**

6.8 The Freedom of Information Team Leader is responsible for co-ordinating the work of the FOI Team, as well as monitoring the manner and timescales in which requests for information are dealt with.

6.9 The Freedom of Information Team Leader reports on compliance with the policy and procedures and also provides monthly performance reports.

6.10 The Freedom of Information Team Leader also:

6.10.1 Provides training and guidance on FOI policy and procedures;

6.10.2 Provides training on issues relating to the Freedom of Information (Scotland) Act, the Environmental Information (Scotland) Regulations and the INSPIRE (Scotland) Regulations; and

6.10.3 Administers the Council's publication scheme.

**Review Officer**

6.11 To ensure impartiality, reviews of decisions where the applicant is dissatisfied with how their response has been dealt with are carried out by the Council's Review Officer.

6.12 The review officer also acts as the liaison link with the Scottish Information Commissioner's office and provides submissions to the Scottish Information Commissioner in relation to any appeals made by dissatisfied applicants.

**Staff**

6.13 All Council staff will:

6.13.1 Be aware of the requirements of the Freedom of Information (Scotland Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009 and what these mean;

6.13.2 Be able to identify any request that falls under the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009;

6.13.3 Provide advice and assistance to persons making requests for information;

6.13.4 Know to pass any information request onto the Information Governance Unit; and

6.13.5 Manage recorded information they hold in accordance with the procedures for records management.

6.14 Some Council staff may be nominated contacts within their service area for providing information to the Information Governance Unit to assist them with the provision of responses to requests. These nominated contacts are also asked to notify the Information Governance Unit of any sensitivity or confidentiality surrounding information covered by the information request.

6.15 Where a nominated contact within a service area is asked to provide information to the Information Governance Unit to assist them with the provision of responses to requests, any such response will be signed off by a manager prior to this being passed to the Information Governance Unit.

6.16 Council staff will be given awareness, induction and update training on the requirements of the Act and Regulations, as appropriate.

# Related documents

7.1 Information Governance Strategy
7.2 Information Governance Policy
7.3 Records Management Policy
7.4 Freedom of Information Policy
7.5 Data Quality Policy
7.6 ICT Acceptable Use Policy
7.7 Open Data Policy
7.8 Employee Code of Conduct

# Equalities impact

8.1 There are no equalities issues arising from this policy.

# Sustainability impact

9.1 There are no sustainability issues arising from this policy.

# Risk assessment

10.1 The risks of not implementing this policy include:
10.1.1 Distress or harm to individuals or organisations.
10.1.2 Reputational damage to the Council.
10.1.3 Non-compliance with legislation.

# Review

11.1 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 Council and presented to Council committee annually, in line with the Council's Policy Framework.

# Appendix 6 - Records Management Policy

## Policy statement

1.2 Council records are sources of administrative, evidential and historical information necessary for the effective functioning and accountability of the Council. Over time they also will provide valuable evidence and understanding of the communities it serves.

1.3 In order for the value of Council records to be maintained and assured, they need to be managed efficiently, transparently and consistently throughout their life-cycle; from the point they are created or received, through maintenance and use, to the time they are destroyed or permanently preserved as archival records.

1.4 This policy sets out the Council's responsibilities and activities in regard to this records management. It governs the management of all records created or acquired on the Council's behalf in the course of Council business.

1.5 This policy:

1.5.1 provides the baseline requirements for good records management within the Council to ensure records are created, managed and used effectively and efficiently;

1.5.2 supports the Council in complying with its statutory and regulatory obligations as well as its commitments as set out in its Information Governance Policy;

1.5.3 defines records management responsibilities throughout the Council;

1.5.4 underpins a working culture which acknowledges the value and benefits of accurate record creation and effective management; and

1.5.5 encourages a leaner Council that retains records for only as long as required for business purposes.

## Scope

2.5 This policy applies to:

2.5.1 All records which are created received and managed in the course of City of Edinburgh Council ('the Council') business ('Council records').

2.5.2 All permanent and temporary Council employees, volunteers, people on work placements and elected members when acting as officers of the Council

2.5.3 All third parties and contractors performing a statutory Council function or service

# Definitions

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

3.2 **Business Unit**: is a term used for teams and sections below that of the Service Area within the Council reporting structure

3.3 **Council Records:** are defined as;

3.3.1 recorded information in any format (including paper, microform, electronic and audio-visual formats); and

3.3.2 which are created, collected, processed, and/or used by City of Edinburgh Council employees, Elected Members when undertaking Council business, predecessor bodies (e.g. Lothian Region Council, Edinburgh District Council, Edinburgh Corporation) or contractors performing a statutory Council function or service.

3.3.3 and which are then kept as evidence of that business.

3.4 **File Plan** is a governance tool that classifies Council records in terms of Council function and activity; it acts as the baseline to connect this policy, and its related guidance and procedures, to the business processes that create, manage, use and dispose of Council records.

3.5 **Format** is the medium is which records are created from; most electronic formats are capable of being edited and changed continually (e.g. MS Word), 'fixed formats' do not allow this (e.g. PDF).

3.6 **Information asset owners:** senior officers involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

3.7 The **Information asset register** is a governance tool that lists the Council's key information assets.

3.8 **Public Records (Scotland) Act 2011:** requires public authorities to detail their records management policies, procedures and responsibilities in a Records Management Plan, which is subject to review by the Keeper of the Records of Scotland.

3.9 **Records management:** are the 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, statutory requirements and policy obligations.

3.10 **Records management manual** – a document that details how records are created, maintained and disposed of within a business unit, service area, project or working group.

3.11 **Recordkeeping systems:** are physical filing systems or IT business systems that hold and manage Council records.

3.12 **Retention Rules:** identify when closed records or files can be disposed of and what should happen to them at that point. They can be broken down into four parts;

3.12.1 Activity / Record Description – provides the context on what is covered by the retention rule.

3.12.2 Trigger – indicates the moment that the retention period starts applying; usually around the event or date that "closes" a record.

3.12.3 Retention Period – how long you hold onto a record beyond the trigger point.

3.12.4 Disposal Action – the action required once a record has reached the end of its retention period.

3.13 **Vital records:** are records classified as being essential to the continuation of Council business.

# Policy content

4.1 To ensure effective management, it is essential that the following policy requirements are understood and applied consistently by all Council employees and services.

4.2 **Creation**

4.2.1 The City of Edinburgh Council is the owner of all Council records, including those created by Elected Members, contractors or consultants.

4.2.2 Council records must be accurate, authoritative and comprehensive in content in order to provide reliable evidence of Council business.

4.2.3 Council records must be titled and referenced in a manner consistent and relevant to the business activity to ensure that they can be easily retrieved, understood and managed.

4.2.4 Council records should be created in fixed formats where ever possible.

4.3 **Storage**

4.3.1 Council records must be adequately protected and stored securely to prevent unauthorised access.

4.3.2 Electronic Council records must be stored on the Council's network in folder structures that conform to the Council's File Plan, or in valid electronic record keeping systems.

4.3.3 Physical Council records no longer needed for immediate or routine use should be sent to the Council's Records Centre for storage and management.

4.3.4 Council records must always be retrievable for business, performance, audit and public rights of access purposes up until they are destroyed.

### 4.4 **Management**

4.4.1 Council records must have access controls and audit logging in place that are appropriate to the sensitivity and risk of their content.

4.4.2 Council records must remain accessible and usable for as long as they are required to be retained under the Council's Retention Schedules.

4.4.3 Council records that are vital to the continuity of Council business must be identified as Vital Records by the business units that hold them.

4.4.4 Council records must not be distributed or copied unnecessarily.

### 4.5 **Disposal**

4.5.1 No Council record may be destroyed without appropriate authorisation and due regard to legal obligations.

4.5.2 All destructions of Council records must be logged by the disposing business unit. This log must be kept for no less than 20 years on a rolling basis.

4.5.3 Council records must be destroyed securely, in compliance with the Council procedures.

4.5.4 Each Directorate will have an authorised Retention Schedule that details how long records of its services and activities should be retained for.

### 4.6 **Transfer to Archive**

4.6.1 Council records identified as having enduring evidential or historical value are to be transferred to the professional care of Edinburgh City Archives for permanent preservation after they have ceased to be of business use.

4.6.2 Records from the Council's predecessors (e.g. Edinburgh District Council, Edinburgh Corporation, civil parishes etc.) must also be transferred to Edinburgh City Archives.

4.6.3 Council records in the care of Edinburgh City Archives will be stored, arranged, described, indexed and made accessible in accordance with professional archival standards and recommendations.

### 4.7 **Records Management Manuals**

4.7.1 Every business unit will have Records Management manuals that document the administrative procedures around Council business activities, dictating who, when and how records are to be created, stored, managed and disposed or transferred.

4.7.2 Records management manuals must be developed locally within the Council services they cover but they should be approved by a relevant working group, or management team as complying with Council policies, regulatory guidance and statutory requirements.

4.7.3 Managers will routinely review their records management manuals and these will also be subject to corporate assessment and audit.

4.7.4 As part of contract due diligence and monitoring, third parties and contractors will be asked to provide similar documentation for their own administrative procedures around the Council records they will create or receive and then manage.

### 4.8 Public Records (Scotland) Act, 2011 – Records Management Plan

4.8.1 The Council commits to submitting and annually reviewing its Records Management Plan, as per statutory requirements set out in the Public Records Scotland Act, 2011.

4.8.2 The Records Management Plan will be developed and reviewed by the Information Governance Unit in conjunction with other relevant officers and overseen by the Information Council.

4.8.3 The draft or reviewed Plan will be approved by Council Management Team and signed off by the Chief Executive before being submitted to the Keeper of the Public Records of Scotland.

# Implementation

5.1 This policy will be implemented through the Information Council's annual plan.

5.2 The initial key measurement of success will be the development and maintenance of records management manuals across the Council but other success measurements will be;

5.2.1 the ongoing management and consistent use by staff of the Council's Retention Schedules

5.2.2 the development, approval and maintenance of the Council's File Plan

5.2.3 the approval of the Council's Records Management Plan by the Keeper of the Public Records of Scotland

5.2.4 the development and roll out of records management training by the Information Governance Unit for staff

5.3 The Information Governance Unit will conduct rolling and periodic reviews of records management manuals and compliance with this Policy within service areas. Results of these assessments will be provided to the relevant Directorate Records Officer and to the Information Council, when and where required.

5.4 Separately, Council IT systems that create and manage electronic records will be subject to assessment by the Information Governance Unit and ICT Solutions to identify and help manage any information risks. Results of these assessments will be reported to the relevant Information Asset Owners and to the Information Council.

# Roles and responsibilities

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to managing Council records.

6.2 The **Chief Executive** has overall executive responsibility for the Council's records policy and for supporting its application throughout the organisation**.** The Chief Executive is also responsible for the management of the City of Edinburgh Council's records under section 1(2a) of the Public Records (Scotland) Act, 2011.

6.3 **Directors** have a general responsibility to ensure that records within their Directorate are managed according to statutory responsibilities and Council policies. They must do this by ensuring that;

6.3.1 there is an up to date, authorised, comprehensive and relevant retention schedule for their directorate

6.3.2 records management manuals are issued and reviewed within their service areas

6.3.3 they have at least one officer fulfilling the role of a Directorate Records Officer

6.3.4 ensuring contracts with third parties performing a public function contain appropriate clauses on expected records management behaviour

6.4 The **Director of Corporate Governance** as the **Senior Information Risk Owner** (SIRO) has the delegated responsibility to authorise, in conjunction with each Director, retention schedules that define how long records should be

retained and what should happen to them subsequently. The Governance Manager is the Deputy SIRO and will act on the Director's behalf as and when required.

6.5 All **Managers** must;

6.5.1 ensure that this policy and any associated records management procedures and guidance are understood by all staff within their business units and that these are incorporated in routine administrative practices

6.5.2 ensure that all administrative practices of their business units are comprehensively documented within records management manuals

6.5.3 maintain a disposal log of all Council records that have been destroyed within their business units on a rolling 20 year basis

6.5.4 identify those Council records that are vital to the continuation of Council business within their records management manuals and inform the Information Governance Unit

6.5.5 consult the Information Governance Unit and their Directorate Records Officer when changes to the Retention Schedules or File Plan are needed to be made

6.5.6 identify and record any existing or emerging risks around Council records on local, divisional and directorate risk registers

6.5.7 undertake annual information governance self assessments to ensure ongoing compliance with this policy and associated information governance activities

6.5.8 provide a statement of assurance to evidence information governance compliance

6.6 **Employees** must;

6.6.1 read, understand and follow this policy and any associated records management procedures and guidance that are relevant to their work

6.6.2 read, understand and follow any records management manuals that are relevant to their work

6.6.3 Identify and report any risks to Council records to their line manager

6.7 **Elected Members** have the same responsibility to manage and dispose of records created in their role as representatives of the Council according to relevant policies and procedures.

6.8 **Third parties (e.g. contractors, voluntary and not for profit organisations) performing a public function for the City of Edinburgh Council** must also

adhere to the requirements set out in this policy and have their own administrative practices documented and assessed in similar ways to Council business units as part of the tendering and contract monitoring processes. To do this they must allow access by relevant Council staff to any Council records they create, receive or manage, including any records keeping system they may hold them in.

6.9 **Directorate Records Officers** will;

6.9.1 have delegated authority to take action and make decisions on records management issues within their directorate.

6.9.2 monitor the administrative practices and records management manuals of their directorate, as well as their directorate retention schedule.

6.9.3 act as a liaison with the Information Governance Unit on records related projects and issues.

6.10 The **Information Governance Unit** is part of the Governance Service with responsibility for the day to day operation and delivery of information governance within the Council. In relation to records management it will;

6.10.1 provide professional guidance, advice and support on the management of Council records for all Council directorates;

6.10.2 create, maintain and renew training modules and toolkits as appropriate;

6.10.3 provide assurance by review of records management manuals;

6.10.4 develop and maintain the Council's File Plan;

6.10.5 maintain and review the Council's Retention Schedules;

6.10.6 oversee the running of the Council's Records Centre;

6.10.7 develop, implement and maintain the Council's Records Management Plan; and

6.10.8 carry out information governance assessments.

6.11 **Edinburgh City Archives** is specifically designated the place of deposit for Council records required for permanent preservation, whether for business or cultural purposes. It is responsible for preserving, promoting and making accessible these records, and other historical records that may be acquired by the Council.

6.12 **ICT Solutions** has a role to support the assessment of existing Council recordkeeping systems against this policy as well as helping to ensure that records management requirements are properly considered as part of the ICT procurement process.

# Related documents

7.1 **Council Policy**

7.1.1 Information Governance Strategy
7.1.2 Information Governance Policy
7.1.3 Open Data Strategy
7.1.4 Data Protection Policy
7.1.5 Data Quality Policy
7.1.6 Freedom of Information Policy
7.1.7 ICT Acceptable Use Policy
7.1.8 Employee Code of Conduct

7.2 **Legislation & Statutory Codes of Practice**

7.2.1 Local Government (Scotland) Act,1994
7.2.2 Data Protection Act, 1998
7.2.3 Public Records Scotland Act, 2011
7.2.4 Code of Practice on Records Management issued under Section 61 of the Freedom of Information (Scotland) Act, 2002

7.3 **Standards**

7.3.1 *ISO 30300 & 30301 – Management Systems for Records;* establishes a model of best practice and assessment for records management within organisations, covering; policy development, statutory and regulatory awareness, responsibilities, process design and performance measuring.

7.3.2 *ISO 15489:2001 – Information and documentation; Records management*; sets out standard terminology, concepts and requirements for records management

# Equalities impact

8.1 There are no equalities issues arising from this policy.

# Sustainability impact

9.1 There are no sustainability issues arising from this policy.

# Risk assessment

10.1 Risk of reputational damage and audit complications as a result of non-compliance with the Public Records (Scotland) Act, 2011.

10.2 Risk of monetary penalties and reputational damage through limited capability to identify and address statutory non-compliance with the Data Protection Act,

1998; specifically Principles 3 (Adequate, relevant and not excessive), 4 (Accurate and maintained), 5 (Over retention) and 7 (Unauthorised access and processing).

10.3 Risk of civil and criminal penalties as a result of a failure to identify and address non-compliance with other legislation that have requirements around records including, but not limited to, education, employment, finance, governance, health & safety and social care.

10.4 Risk of civil and criminal penalties as well as reputational damage and business continuity issues through poor decision making and accountability based on inadequate and poorly managed Council records.

10.5 Risk of weak internal governance and audit complications through a failure to raise and maintain the awareness of Council staff of records management requirements, best practice and standards.

10.6 Risk of excessive physical and IT storage costs through a failure to identify and apply appropriate retention rules to Council records.

10.7 Risk to citizens and clients that the Council will mismanage their service provision due to inadequate and poorly managed Council records.

# Review

11.2 In line with the Council's Policy Framework, this policy will be reviewed annually or when required by significant changes to the Council's Records Management Plan or with legislation, regulation or business practice.