Corporate Policy and Strategy Committee

10am, Tuesday, 4 October 2016

Information Governance Policies

Item number	7.1
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's Information Governance Policy suite has been added to and revised to help ensure compliance with legislative, regulatory and best practice standards, and to promote a culture of openness and transparency.

Links

Coalition pledges	
Council outcomes	
Single Outcome Agreement	

Report

Information Governance Policies

Recommendations

1.1 To approve the Information Governance policies set out in appendices 2 to 9 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 that the Council has to operate in. Appendix 1 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 UK Information Commissioner. The latter, in particular, has a wide range of enforcement powers where organisations have been found to breach the Data Protection Act 1998. 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 during 2016.

2.4 Information governance is a collection of controls and assurance that provide a coherent, multidisciplinary, approach and structure to the Council's efforts in meeting its legislative and regulatory requirements around its information, while also encouraging the adoption of standards and best practice on an improvement model basis. It covers the use and development of the Council's archives, the quality of its data, the information rights of its citizens, the security of its information, how it processes personal data, how it manages its records, and how it makes its information available for re-use. Overall, it ensures that the Council is creating, managing, using, sharing and disposing of information efficiently, appropriately and lawfully.

2.5 Since the initial approval of the Council's Information Governance Policy suite in 2014, the Council's developing information governance arrangements have been subject to:

2.5.1 extensive scrutiny from internal and external auditors (e.g. UK Information Commissioner's audit of the Council's data protection arrangements);

2.5.2 legislative changes (e.g. revised re-use of public sector information regulations and the Public Bodies (Joint Working) Scotland Act 2014);

2.5.3 formal approval processes required under legislation (e.g. Council's Records Management Plan); and

2.5.4 Scottish Government initiatives (e.g. Open Data).

2.6 The Information Governance Unit, which has responsibility for the day to day operation of information governance within the Council, has been through an organisational review as part of the Council's transformation process during 2016. The revised structure provides a more flexible and responsive approach to information governance, with a renewed emphasis on information risk and assurance. Data quality issues are also being actively addressed through the creation of the Data Services Team under the Strategy & Insight Division.

2.7 The issues outlined above have required significant policy review and revision to reflect change and new priorities. These are set out in more detail in the policy descriptions below.

2.8 To provide a more comprehensive approach to information governance, new policy areas have been added to the suite of policies around archives, information security and the re-use of public sector information.

Main report

3.1 Each Information Governance area has a top level policy, outlined in the paragraphs below. Each policy clearly sets out roles, responsibilities and requirements to ensure compliance with relevant legislation, regulation, standards and best practice.

Information Governance Policy (Appendix 2)

3.2 This policy sets out the Council's over arching governance arrangements to ensure that information is effectively managed and properly protected. It clearly defines the roles and responsibilities of all stakeholders who are involved in handling and managing Council information, especially around information risk and information asset management. It has been revised to reflect organisational changes within the Council.

Archives Policy (Appendix 3)

3.3 This new Archives Policy sets out the Council's responsibilities and activities in regard to its archives, which are a unique and valuable resource that documents and represents the changing nature of the city over time. They provide the Council with its corporate memory and help to enhance civic and community identity, support long term accountability, and document and protect the rights of citizens.

3.4 The policy details the collection, management, preservation and access arrangements of all archives, both physical and digital, created or acquired by the Council. It also supports the Council in complying with its statutory, regulatory and policy obligations around archives, and is an integral part of the UK National Archives Archive Services Accreditation standard.

Data Quality Policy (Appendix 4)

3.5 This policy confirms the Council's commitment and approach to improving the quality of its data. The policy has been significantly revised to reflect organisation change and the creation of a Data Services Team within the Strategy and Insight Division. The new team will provide specialist data analytical resources and services, and will help to implement the quality principles and objectives detailed in this policy through the development of Quality Action Plans. In particular, a framework of management arrangements will be developed to assure partners and other stakeholders that the quality of the Council's data is reliable and sustainable.

Information Rights Policy (Appendix 5)

3.6 This policy replaces the previous Freedom of Information Policy and formalises the Council's approach to promoting and facilitating the information rights of individuals. While it continues to set out the Council's arrangements for disclosing information under Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, and the INSPIRE (Scotland) Regulations 2009, the Information Rights Policy also incorporates information access and processing rights under the Data Protection Act 1998 and the Pupils' Educational Records (Scotland) Regulations 2003.

3.7 The inclusion of all information regimes in one policy provides a more coherent and comprehensive approach in helping individuals exercise their statutory rights. It also helps to evidence the Council's commitment to openness, accountability and transparency about its actions and how it operates.

Information Security Policy (Appendix 6)

3.8 The Council depends on the confidentiality, integrity and availability of its information to deliver services. It also has statutory responsibilities to make sure that the data and information it creates or receives is kept safe and used appropriately.

3.9 In setting out the Council's information security arrangements, this new policy confirms the Council's commitment to its citizens, visitors, employees and business partners that Council information and data will be properly protected, valued and secured.

Managing Personal Data Policy (Appendix 7)

3.10 A new Managing Personal Data Policy has been created to encompass recommendations made by the UK Information Commissioner's Office, following an audit of the Council's data protection arrangements during 2015-2016. It replaces the previous Data Protection Policy and formalises the Council's

approach to managing personal data in accordance with the requirements of the Data Protection Act 1998, and outlines the Council's commitment to the principles enshrined within the Act.

3.11 The policy acknowledges the need to balance the rights of individuals with the functions and operational requirements of the Council, and also anticipates the introduction of the General Data Protection Regulation in 2018. In particular, it recognises the more robust approach that will be required in relation to fair processing and consent.

Records Management Policy (Appendix 8)

3.12 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. The policy has been significantly revised to reflect the Council's approved Records Management Plan: a key statutory requirement under the Public Records (Scotland) Act 2011.

Re-use of Public Sector Information Policy (Appendix 9)

3.13 The Re-use of Public Sector Information Regulations 2015 provides a legal framework to encourage the re-use of public sector information. This is a new policy which formalises and sets out the Council's approach and arrangements to complying with the Regulations, and reaffirms the Council's commitment to open data and the proactive publication whenever possible.

Implementation and compliance

3.14 These policies set out the organisational commitment to meet the Council's legislative and regulatory requirements around its information, as well as to continuously improve how its information is used and managed. However, to ensure effective compliance, related guidance and procedures, communications and training are all needed to turn these commitments into tailored messages and approaches for staff to adopt and incorporate into their daily work and behaviour.

3.15 Several procedures and a range of guidance have already been developed and made available on the Council's intranet to support staff in implementing and complying with these policies. These are outlined in each individual policy but many of them are in the process of being revised and expanded upon by the Council's Information Governance Unit to reflect changes in Council structure, policy and legislation.

3.16 There is also a new emphasis on encouraging the development or updating of local documentation across the Council to embed and localise compliance with these policies. This supports both the Council's need for greater flexibility in front line service delivery by allowing localisation, as well as meeting the increasing challenge from external regulators for documentary evidence of compliance. The aim is to first encourage the documenting of existing local information governance arrangements, and then for the Council's Information Governance Unit to review these as a consensual follow up process of advice and assurance.

3.17 While staff responsibilities are set out in these policies in broad and general terms, there is also an information governance communications plan that identifies specific messages for different areas and levels of staff, to be reached through a variety of channels and at different times. These messages remind staff in a concise, relevant and timely fashion about their particular roles in managing Council information. The communications plan is refreshed on an annual basis and is developed between the Information Governance Unit and the Communications Service.

3.18 Awareness raising, through events such as Global Information Governance Day (16 February 2017), will provide opportunities to highlight the Council's commitments to managing its information effectively beyond simply policy and procedure. However, at a more routine level, there is already a mandatory information governance e-learning module for all staff to complete that collates together basic elements of compliance and good practice from all of the policies. Further e-learning content and training materials to highlight certain themes and target specific staff groups are currently being developed and piloted by the Information Governance Unit and Human Resources. These will be aligned to the Council's evolving induction and learning framework.

3.19 All of this is in addition to the daily advice and support already provided by the Information Governance Unit to colleagues and members of the public in relation to the management and use of Council information.

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 is being 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 relevant service areas across the Council.

Background reading/external references

Data Protection Act 1998

Freedom of Information (Scotland) Act 2002

Environmental Information (Scotland) Regulations 2004

INSPIRE (Scotland) Regulations 2009

Public Records (Scotland) Act 2011

Office of the Scottish Information Commissioner

Information Commissioner's Office

Archives Services Accreditation

National Records of Scotland

Guide to the Re-use of Public Sector Information Regulations 2015

Guide to the Pupils' Educational Records (Scotland) Regulations 2003

City of Edinburgh Council's Records Management Plan

Andrew Kerr
Chief Executive

Contact: Kirsty-Louise Campbell, Head of Strategy & Insight (Interim)

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

Contact: Kevin Wilbraham, Information Governance Manager

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

Links

Coalition pledges

Council outcomes

Single Outcome Agreement

Appendices:

Appendix 1 – Information Legislation

Appendix 2 – Information Governance Policy

Appendix 3 – Archives Policy

Appendix 4 – Data Quality Policy

Appendix 5 –Information Rights Policy

Appendix 6 – Information Security Policy

Appendix 7 – Managing Personal Data Policy

Appendix 8 – Records Management Policy

Appendix 9 – Re-use of Public Sector Information Policy

Appendix 1

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
2014 asp. 09 Public Bodies (Joint Working) (Scotland) Act 2014
Key Statutory Instruments of the UK Parliament
S.I. 2015 / 1415 The Re-use of Public Sector Information Regulations, 2015
Key Statutory Instruments of the Scottish Parliament
S.S.I. 2003 / 581 The Pupil's Educational Records (Scotland) Regulations
S.S.I. 2004 / 520 Environmental Information (Scotland) Regulations
Key Statutory Codes of Practice
Section 60 Code of Practice: Function under FOI(S)A

Section 61 Code of Practice: Records Management and FOI(S)A
Key International & British Standards
ISO 15489: 2001 Information and Documentation - Records Management
ISO 16175 Principles and functional requirements for records in electronic office environments
ISO 23081 Metadata for records
ISO 27000 series – Information Security Management System
ISO 30300 series – Management Systems for Records

Appendix 2 – Information Governance Policy

Implementation date:

Control schedule

Approved by	Corporate Policy and Strategy Committee
Approval date	
Senior Responsible Officer	Jo McStay, Strategy and Insight Senior Manager
Author	Kevin Wilbraham , Information Governance Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	05-09-2014	Kevin Wilbraham	Circulated for comment; changes incorporated
0.2	17-09-2014	Kevin Wilbraham	Agreed by Information Council
1.0	30-09-2014	Kevin Wilbraham	Agreed by CP&S
1.1	03-08-2016	Kevin Wilbraham	Revised to reflect organisational change and audit recommendations; circulated for comment
1.2	01-09-2016	Kevin Wilbraham	Changes incorporated from Head of Strategy (Interim)
1.3	03-09-2016	Kevin Wilbraham	Revised draft agreed with Head of Strategy (Interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30-09-2014	Corporate Policy & Strategy	Information Governance Policies	Minute

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 (hardcopy and electronic);

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

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

Definitions

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

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

3.3 **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.

3.4 **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**.**

3.5 **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.

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

3.8 **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.

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

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

3.11 **Organisational controls**: are measures that instruct and define responsibilities and expected behaviours and practices in terms of information security (e.g. policies, procedures, guidance)

3.12 **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.

3.13 **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.

3.14 **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.

3.15 **Technical controls**: are measures that limit and define access and action via network and system configuration in terms of information security (e.g. account management, back up cycles, encryption and firewalls)

3.16 **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 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 1 details the many acts, regulations, codes of practice and technical standards concerning IG.

4.4 Good information governance improves, monitors and provides assurance that the Council is creating, managing, using, sharing and disposing of information efficiently, appropriately and lawfully.

Information governance framework

4.5 The Council has developed an Information Governance Framework that brings together all the legislative and regulatory requirements, standards and best practice in relation to the following areas:

4.5.1 Data quality

4.5.2 Information compliance

4.5.3 Information rights

4.5.4 Information security

4.5.5 Records and archives management

4.5.6 Re-use and open data

Policies

4.6 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 Council Leadership Team and Committee.

Procedures

4.7 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

4.8 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.

4.9 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 for each IG area will be developed and delivered by the relevant Council team.

Communications

4.10 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

4.11 The Information Governance Unit will facilitate regular and effective monitoring to support the implementation and assessment of IG practices and behaviours across the Council.

4.11.1 An annual IG self-assessment programme will be undertaken by Council managers and overseen by the Information Governance Unit. The results of this assessment will be presented to the Information Council and inform the themes and priorities of the following year's IG annual action plan.

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

Information asset register

4.12 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 management

4.13 The Information Governance Unit will support managers in identifying, reporting and managing information risks within the Council's wider Risk Management Framework.

4.14 The Council's risk management committees will also receive support and input from the Information Governance Unit in considering information risks.

4.15 The Information Council will receive and act upon reports of collated information risks brought together by the Information Governance Unit on a routine basis.

Information incident reporting

4.16 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 captured and managed in the appropriate risk registers.

Privacy impact assessments

4.17 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

4.18 An information governance maturity model will be used by the Information Council to determine progress against this policy and related policies and external standards. Overall success will be determined by improvement in information governance maturity over a five year period.

Annual report

4.19 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

4.20 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. The plan will outline key tasks, outcomes, accountabilities and progress.

5.2 Key measurements of success will be:

5.2.1 Roll out and maintenance of an annual maturity assessment programme

5.2.2 Continued development and maintenance of the Council's Information Asset Register

5.2.3 Continued roll out of training, guidance and internal communications to raise and underpin awareness IG requirements and best practice

5.2.4 Routine reporting of information breaches and risks with follow up and mitigating actions

5.2.5 Maintenance and development of IG controls, as outlined in related policies

Roles and responsibilities

Council Leadership Team

6.1 The Chief Executive and Directors have specific responsibilities in the related IG policies but more widely, the Council Leadership Team has overall collective 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 Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation. Specific responsibilities include:

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

6.3.2 Chairing the Information Council to lead and coordinate information governance improvements throughout the organisation.

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

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

6.3.5 Owning the organisation's information incident management framework

6.3.6 Providing the final point of resolution for any information risk issues.

Information Governance Manager (Deputy Senior Information Risk Owner)

6.4 Accountability for the on-going strategic development of information governance lies with the Information Governance Manager within the Strategy and Insight service area of the Chief Executive's Office. The Information Governance Manager deputises for the SIRO as required and 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 Council Leadership 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. The IC reports to Council Leadership Team and Committee through the Council's SIRO.

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 Implementing and supporting the IC's annual action plan.

6.7.2 Developing, assessing and reporting on IG maturity within service areas against the Council's IG maturity model.

6.7.3 Collating and presenting analysis of key performance data around information governance to senior managers.

6.7.4 Annually reviewing and updating the Council's suite of information governance policies.

6.7.5 Developing and providing practical IG guidance and training for service areas.

6.7.6 Providing a focal point for all IG enquiries.

6.7.7 Liaising with external regulators and leading on or supporting resolution of compliance issues, as appropriate.

6.7.8 Collating and responding to requests for information under access legislation.

6.7.9 Developing and maintaining the Council's IG tools and standards, including its Information Asset Register, Business Classification Scheme and Record Retention Schedule.

6.7.10 Developing and maintaining a register of the Council's information sharing protocols and agreements.

6.7.11 Assessing, reporting on and improving organisational controls for information security in line with ISO/IEC 27001:2013 – Information Security Management and other compliance frameworks.

6.7.12 Receiving and managing relevant breach and incident reporting and ensuring remedial actions have been undertaken.

6.7.13 Preserving and providing access to the Council's archives.

ICT Solutions

6.8 ICT Solutions is the operational lead on technical IT risks and is responsible for implementing appropriate technical controls for information security, in line with

ISO/IEC 27001:2013 – Information Security Management and other compliance frameworks (e.g. the Public Services Network).

6.9 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.

6.9.2 Integrating information governance into local processes to ensure that there is on-going compliance on a day to day basis.

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

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 ICT Acceptable Use Policy

7.4 Information Rights Policy

7.5 Information Security Policy

7.6 Managing Personal Data Policy

7.7 Records Management Policy

7.8 Re-use of Public Sector Information Policy

Codes, Guidance, Procedures and Strategy

7.9 Employee Code of Conduct

7.10 Role guidance for Information Asset Owners and Data Stewards

7.11 Information Risk Management guidance

7.12 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 3 – Archives Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Kevin Wilbraham, Information Governance Manager
Author	Henry Sullivan, Information Asset Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	15-07-2016	Henry Sullivan	Original Draft – combining existing draft policies for Collections Development and Collections Information
0.2	15-08-2016	Henry Sullivan	Substantial re-write
0.3	15-08-2016	Kevin Wilbraham	Minor revisions and additions made
0.4	03-09-2016	Kevin Wilbraham	Revised draft agreed with Head of Strategy (Interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30-09-2014	Corporate Policy & Strategy	Information Governance Policies	Minute

Archives Policy

Policy statement

1.1 The City of Edinburgh's archives form a core part of the documented heritage of the city that stretches back to the 12th century to the present day. The archives illuminate our past, chronicle our present and inform our future.

1.2 When properly managed and made accessible, the Council archives will enhance civic and community identity, support long term accountability, and document and protect the rights of citizens.

1.3 To be effective, the Council archives need to evolve over time to capture and represent the changing nature of the organisation and city, as well as the changing ways we create records in the ongoing digital revolution.

1.4 This policy sets out the Council's responsibilities and activities in regard to its archives. It governs the collection, management, preservation and access of all archives, both physical and digital, created or acquired by the Council

1.5 This policy will:

1.5.1 define managerial and professional responsibilities for the Council archives;

1.5.2 support the Council in complying with its statutory, regulatory and policy obligations around archives,

1.5.3 acknowledge the value and benefits of an archive service for the Council as a custodian of the city's culture and history, for our citizens as its inheritors and continuators and for our visitors who come to experience and contribute to it.

Scope

2.1 This policy covers:

2.1.1 All records which are created or received and then managed by the Council in the course of its business.

2.1.2 All records which were created or kept by the Council's predecessor bodies.

2.1.3 Any archives purchased by any service area in the Council

2.1.4 Any archives donated or deposited with any service area in the Council by third parties

2.2 This policy applies to:

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

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

Definitions

3.1 **Appraisal:** is the assessment of records for their enduring business, evidential or historical value to the Council or communities it serves.

3.1.1 Records that are assessed to have value are retained as **Archives**.

3.1.2 Records that do not have sufficient value are either disposed of or returned to their depositor.

3.2 **Conservation:** is the active repair or restoration of damaged archives.

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 **Depositor:** the person or organisation that transfers custody of records to an archive institution. These **deposits** fall under one of five types:

3.4.1 **Charge and Superintendence:** records that have been transferred to the Council from the National Records of Scotland as part of a national scheme to support local archive services. These records are still owned by their depositors but the National Records of Scotland maintains a supervisory role on how they are accessed and managed locally.

3.4.2 **Gift***:* a permanent transfer of ownership of records. Legal ownership, responsibility and rights, both physical and intellectual, are entirely consigned to the Council.

3.4.3 **Loan**: the Council is the custodian for the records but is not the legal owner. This is usually the Depositor but may be another nominated individual or official of a business or institution. Some loans are **indefinite** where the records are managed by the Council until the depositor wishes to withdraw them. Other loans are **temporary**, where the Council has the records for a fixed period of time, often for exhibition purposes.

3.4.4 **Purchase:** the Council has acquired the records through sale directly or indirectly from the legal owners. Some intellectual rights may not be acquired as a result of the purchase.

3.4.5 **Transfer:** records that have been created by the Council and which have been moved to the Council archives after being appraised as having enduring business, evidential or historical value.

3.5 **Format** is the medium from which records are created; 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 **Preservation:** is a set of processes that prolong the life of archives through identifying risks to their continued access and use and then mitigating them through management action.

3.7 **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.

3.8 **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.

3.9 **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.

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

3.11 **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;

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

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

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

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

Policy content

4.1 The Council has the duty and powers to manage, preserve and provide access to any records of local or general historic interest that have been created or received by it, or otherwise placed in its custody by way of gift, purchase, loan or transfer.

4.2 The Council's Records Management Plan, under the Public Records Scotland Act of 2011, recognises that the Council's Archives Service (Edinburgh City Archives) is the main place of deposit for these records, though other Council services have and maintain historic records of their own to support their own collections and services. Collectively these are all regarded as the Council's archives.

4.3 The Council's Information Asset Manager is responsible for the Council's archives under Element 7 of the Council's Records Management Plan.

4.4 Edinburgh City Archives is also the custodian of all archives deposited under Charge and Superintendence by the Keeper of the Records of Scotland.

4.5 A five year Archive Development Plan for the Council will be developed by the Information Asset Manager, in consultation with relevant stakeholders, and presented to and approved by the Information Council.

4.5.1 Its purpose will be to assess, consult on, and set out how the Council's archives can be developed to better meet the needs of existing and potential stakeholders and communities.

4.5.2 It will cover the Council archives' acquisition and appraisal priorities, as well as access, engagement and management arrangements across the organisation.

Acquisitions

4.6 The Council will seek to add its archives by:

4.6.1 Responding to offers of material from institutions, businesses and individuals, including additional deposits from existing depositors.

4.6.2 Identifying and pursuing material that fills gaps in its archives or falls within the Council's Archives Development Plan.

4.7 This will be done in liaison with other Council service areas (as appropriate) and external bodies, including the National Records of Scotland, the other Lothian local authorities, and other relevant national and local repositories.

4.8 The Council will not seek to represent any particular historical, sectarian or other viewpoint in its acquisition of archives, but shall reflect, as accurately as possible, all aspects of Edinburgh's past and present.

4.9 In acquiring archives, the Council will adhere to the following priorities:

4.9.1 Records of the City of Edinburgh Council and its predecessors which relate to their core functions and statutory duties.

4.9.2 Records of Arms Length External Organisations created or contracted by the Council

4.9.3 Archives of the Burghs of Leith, Portobello, South Queensferry and all related Parish Councils, Parochial Boards, District Councils, School Boards etc.

4.9.4 Archives of Edinburgh institutions and businesses and those of religious, sporting, political or cultural organisations and families or individuals which merit preservation.

4.9.5 Archives of regional bodies which have or did have their headquarters in Edinburgh except where provision has already been made or agreed with another repository.

4.10 Archives that fall within the above criteria but are in danger of neglect or destruction should be particularly sought after and secured.

4.11 The Council will always seek the return into Council custody of any archives of the City of Edinburgh Council and its predecessor and associated bodies currently held in other institutions and agencies where appropriate.

4.12 Where an acquisition seems likely to result in significant financial implications in respect of storage, conservation or access then the matter should be referred to Council committee.

4.13 The Council will not acquire archive material relating to places outside the Council's geographical area, unless they are part of a wider archive collection that has relevance to Edinburgh.

4.14 Where the Council is offered archives that do not match its acquisition criteria, the potential depositor must be advised so by the liaising Council officer and provided with details of appropriate alternative institutions to consider.

4.15 The Council will, in exceptional circumstances, act to rescue and secure archives for other archival institutions before arranging for their transfer to the most appropriate custodian.

Deposits by gift, loan, purchase or transfer

4.16 Current Council records of archival merit will be transferred over time to the secure custody of Edinburgh City Archives in accordance with the Council's Record Retention Schedule and Archive Transfer Procedure.

4.17 Archives from third parties must always be first sought as gifts in order to provide the citizens of Edinburgh with maximum and enduring value.

4.18 Indefinite loans of archives can be accepted where the depositor wishes to maintain ownership while allowing public access and use.

4.19 Acquisitions by purchases will only be considered by the Council if the material is of outstanding importance to Edinburgh's archival heritage.

4.20 The Council will not accept any archives which have been collected or acquired in any country in violation of that country's laws.

4.21 Archives gained by gift or purchase should have clear title of ownership and these should be transferred to the Council upon acquisition.

4.22 All deposits by loan to the Council will have formal documentation setting out the arrangements and will be signed by all relevant parties.

4.23 Any identified conservation issues of potential loans will remain the liability of the depositor, subject to agreement concerning such matters as payment, withdrawal from access, application for funding etc.

4.24 All archive deposits in the Council's custody will eventually be made available for public consultation, either immediately or at the expiry of specified closure periods agreed with the depositor.

4.25 The Council will not accept any archive deposit with an indefinite or unclear closure period requirement set by a depositor.

Appraisal

4.26 All archive acquisitions will be appraised against the Archives Development Plan in accordance with the Council's Archive Appraisal Procedure before they are formally accepted by the Council. In some cases archives may be returned to the donor or depositor after appraisal, in full or in part.

4.27 All archive deposits must be appraised for compliance with the current legislative regime; e.g. Statute of Limitations, the Data Protection and Freedom of Information Acts, Scottish Public Records Acts.

Accession

4.28 All deposits will be documented within a Council Archives Accessions Register. This will be maintained by the Information Asset Manager.

4.29 Additional acquisition paperwork should be permanently retained by the collecting Council service as appropriate.

4.30 All major accessions to the Council archives will be reported to the National Register of Archives for Scotland and listed in an annual report to the Information Council.

Loans, de-accessions and disposal

4.31 Any Council service that loans out archives in the Council's custody to a third party for exhibition, conservation, or other appropriate purposes, must follow the Council's Archives Loans Procedure.

4.32 The Council will not transfer (except in case of disaster/emergency), loan, sell or otherwise dispose of any archives under deposit by loan without the owner's written consent.

4.33 Any possible sale, destruction or transfer to a third party of the Council's archives will require authorisation from the Information Asset Manager.

4.34 Whilst depositors may withdraw their deposited or loaned archives from Council custody, the Council reserves the right to:

4.34.1 Claim reimbursement for the time and materials spent in cataloguing and preserving the archive

4.34.2 Retain any catalogues and other finding aids of the archive, as well as any copies made from the archive

4.35 All depositors removing their deposited or loaned archives from Council custody shall receive and sign de-accession documentation.

Preservation and conservation

4.36 All Council archives will be stored in secure and environmentally stable conditions and kept in appropriate low acid packaging, as far as resources will allow.

4.37 All Council archives will be managed as part of a preservation programme to ensure their continued access and use.

4.38 The Information Asset Manager will, in consultation with relevant stakeholders, issue and maintain guidance on the appropriate storage, care and preservation of the Council's archival records.

4.39 This guidance will meet professional archive standards and will cover the continual monitoring of environmental conditions, pest management and control, security and general housekeeping within storage areas.

4.40 Council archives that require external conservation treatment will be repaired in accordance with the Council's archive conservation guidance, issued and maintained by the Information Asset Manager.

4.41 A disaster plan for the Council archives will be maintained by the Information Asset Manager.

Access

4.42 The Council will provide as wide an access to its archives as possible, for both citizen and visitor alike, and for a diverse range of interests and research needs.

4.43 The Council will do this by:

4.43.1 Committing to making all archive material publically accessible as soon as practically possible after their accession.

4.43.2 Providing free physical access to the Council's archives to those who can visit the Council's designated access points

4.43.3 Responding to remote enquiries about the Council's archives.

4.43.4 Publishing catalogues and other finding aids online.

4.43.5 Creating and putting on physical and online exhibitions of material from the Council archives.

4.43.6 Providing a charged research service that takes into account the complexity of research required, and the needs of the enquirer

4.43.7 Digitising archival materials (within budgetary constraints) to provide on-line access to archival collections

4.44 While the Council archives fall under the exemption on research, history and statistics within section 33 of the Data Protection 1998, the Council reserves the right to refuse access to specific archive material due to conservation or privacy concerns. These restrictions will be highlighted in published catalogues and finding aids where ever possible.

Documentation

4.45 All archives acquired by the Council will be catalogued according to the Council's Archive Cataloguing Guidelines.

4.46 These guidelines will be routinely reviewed by the Information Asset Manager, in consultation with other stakeholder services in the Council, and updated in accordance with current professional archives best practice and standards.

Digital Preservation

4.47 The Council commits to developing and maintaining a digital repository to capture, manage and provide long term access to the Council's digital archives.

4.48 Digital Council records that are required for long term (ten years or more) or permanent retention should be kept in robust file formats identified and recommended by the Information Asset Manager.

4.49 Each Council record keeping system that contains information required for long term or permanent retention should have a digital continuity plan

Implementation

5.1 This policy will be implemented through the Information Council's annual plan under the records management stream and coordinated by the Information Asset Manager.

5.2 The Information Asset Manager will undertake assessments of the Council archives throughout the organisation for compliance against this policy and related procedures and guidance.

5.3 Key measurements of success will be:

5.3.1 Number of archive collections accessioned and catalogued

5.3.2 Percentage of uncatalogued archive collections

5.3.3 Number of users of the Council archives

5.3.4 Number of item productions from the Council archives

5.3.5 Number of exhibitions and other outreach activities undertaken to promote the Council archives

5.3.6 User feedback through annual customer surveys

5.3.7 Development of a digital archive repository for the Council – including relevant processes, skill sets, guidance and technical infrastructure

5.4 An annual report to the Information Council by the Information Asset Manager will detail progress and developments in complying with this policy and wider professional archival best practice. It will cover:

5.4.1 Annual performance statistics for the above key measurements of success

5.4.2 Collated assessment of the access, management and preservation arrangements for the Council's archives across the organisation

5.4.3 Disaster plan testing and review

5.5 Achieving and maintaining the UK National Archives' Archive Services Accreditation standard will be the benchmark for the Council in complying with this policy. This accreditation will be managed by the Information Asset Manager and overseen by 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 acquiring, managing, preserving and providing access to the Council's archives.

6.2 The **Chief Executive** has overall executive responsibility for the Council's archives as the senior manager responsible for the Council's Records Management Plan under the Public Records (Scotland) Act, 2011.

6.3 **Directors** have a general responsibility to ensure that records of enduring business, evidential or historical value within their Directorate are identified and eventually transferred to the Archives Service. 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 there are routine transfer arrangements to the Council archives for all activities that have permanent retention rules

6.3.3 digital records that require long term or permanent retention are kept in robust file formats

6.3.4 record keeping systems that require long term or permanent retention of information are identified and digital continuity plans are created and maintained

6.4 The **Head of Strategy & Insight** as the **Senior Information Risk Owner** (SIRO) has the delegated responsibility for information risk management in the

Council, including risks to the permanent preservation and ongoing access to the Council's archives.

6.5 All **Managers** must;

6.5.1 ensure that this policy and any associated procedures and guidance are understood by all relevant staff within their business units

6.5.2 undertake routine transfers to the City archives of any Council records in their custody that have a permanent retention rule

6.5.3 manage the file formats of the Council records in their custody that require long term or permanent retention

6.5.4 consult the Information Governance Unit and their Directorate Records Officer when they believe records due for destruction may have enduring business, evidential or historical value to the Council or communities it serves

6.5.5 not destroy Council records that are being actively considered for appraisal and transfer into the Council archives until given notification by the Information Asset Manager

6.6 **Employees** must;

6.6.1 read, understand and follow this policy and any associated archive 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 the long term preservation and use of Council records to their line manager

6.6.4 Report to their manager any Council records due for destruction that might have enduring business, evidential or historical value

6.7 **Elected Members** have the same responsibility to manage records created in their role as representatives of the Council in accordance with relevant policies and procedures. However, as members of the governing body of the Council, they have a greater duty to ensure that the Council archives remain relevant in terms of content and management – especially in meeting the civic need for accountability and documenting the rights and responsibilities of both the Council and its citizens.

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 where they create records that require permanent retention.

6.8.1 They must transfer these records to Council custody either through an agreed schedule or at the termination of contract.

6.8.2 They must also comply with requests by the Council to transfer other material created under their contract that have been deemed of enduring business, evidential or historical value to the Council and the communities it serves.

6.9 **Directorate Records Officers** will;

6.9.1 have delegated authority to transfer Council records within their directorate to the Council archives.

6.9.2 act as a liaison with the Information Governance Unit on archive and digital preservation related projects and issues.

6.10 The **Council Information Asset Manager** is part of the **Information Governance Unit** within the Strategy & Insight division of the Chief Executive's Office. The position has responsibility for the day to day operation of **Edinburgh City Archives** and for the delivery of the Council's Records Management Plan. In relation to archives this officer will:

6.10.1 provide professional advice, guidance, support and training on the management of the Council archives across the organisation

6.10.2 Develop, maintain and report on the Council's Archive Development Plan;

6.10.3 develop and maintain the Council's Archives Accession Register;

6.10.4 maintain and review the Council's Retention Schedules;

6.10.5 promote and provide assurance by review of preservation programmes for the Council archives by custodial Council service areas;

6.10.6 Review and authorise sales, destructions or transfers of any part the Council archives

6.10.7 Develop, test, review and report on a disaster plan for the Council archives

6.10.8 Lead on and promote digital preservation of Council records and archives, specifically in developing a digital archives repository.

6.11 **ICT Solutions** has a role to support the digital preservation of Council records and record keeping systems required for long term or permanent retention, as well as helping to ensure that digital preservation requirements are properly considered as part of the ICT procurement process.

Related documents

Council Policy

7.1 Data Quality Policy

7.2 Edinburgh Museums and Galleries: Collections Development Policy 2013-2017

7.3 Information Governance Policy

7.4 Information Rights Policy

7.5 Information Security Policy

7.6 Managing Personal Data Policy

7.7 Records Management Policy

7.8 Re-use of Public Sector Information Policy

Codes, Guidance, Procedures and Strategy

7.9 Council Archives Transfer Procedure

7.10 Open Data Strategy

Legislation & Statutory Codes of Practice

7.11 Local Government (Scotland) Act,1994

7.12 Public Records Scotland Act, 2011

Standards

7.13 Archives Service Accreditation Standard of the UK National Archives

7.14 International Standards for Archival Description and Archive Authority Files

7.15 PD5454: 2012 - *Guide for the storage and exhibition of archival materials*

7.16 ISO 14721:2012 - *Open archival information system (OAIS)*

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 and the Council's own Records Management Plan.

10.2 Risk of civil and criminal penalties, as well as reputational damage, as a result poor decision making through a failure to raise and maintain the awareness amongst staff of the evidential value of the Council archives to its current and future business.

10.3 Risk of civil and criminal penalties as well as reputational damage and business continuity issues through an inability to evidence past Council decisions due to inadequate and poorly managed long term access and preservation of Council records.

10.4 Risk of excessive physical and IT storage costs through a failure to identify and make separate provision for Council records that must be retained permanently.

10.5 Risk to citizens and clients that the Council will be unable to evidence any decision making and service provision that have affected them in the long term due to inadequate and poorly managed Council records.

Review

11.1 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.

Appendix 4 – Data Quality Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Edel McManus, Data Services Manager
Author	Edel McManus, Data Services Manager Kevin Wilbraham, Information Governance Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	05-09-2014	Kevin Wilbraham	Circulated for comment
0.2	17-09-2014	Kevin Wilbraham	Agreed by Information Council
1.0	30-09-2014	Kevin Wilbraham	Approved by CP&S
1.1	28-08-2016	Edel McManus	Major revision to reflect organisational change and strategic priorities
1.2	03-09-2016	Edel McManus	Agreed with Head of Strategy (Interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30/09/2014	Corporate Policy & Strategy	Information Governance Policies	Minute

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.

3.8 **Data Warehouse:** a storage architecture designed to hold data extracted from transaction systems, operational data stores and external sources. The warehouse then combines that data in an aggregate, summary form suitable for enterprise-wide data analysis and reporting for predefined business needs. The Data warehouse toolsets will enable data profiling, modelling, analytics and monitoring to support data quality management.

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.

Data Quality Principles

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

4.5.5 **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.

Data Quality Objectives

4.6 The council's corporate objectives for data quality define a framework of management arrangements which will assure partners and other stakeholders that the quality of our data is reliable and sustainable. The council's corporate data quality objectives, together with actions required to achieve them are to:

Appropriate Responsibility, Accountability and Awareness

4.6.1 Every member of staff will recognise the need for good quality data and how they can contribute to it

4.6.2 Every member of staff will be aware of their individual responsibilities with regard to data collection, storage, analysis and reporting

4.6.3 Every member of staff will be aware of the implications of poor data quality in their area in terms of internal and external accountability including those affecting other departments and the Council as a whole

4.6.4 Every member of staff will report any systematic data quality issues immediately to their manager who should ensure remedial action is taken

4.6.5 Every member of staff will be aware of the policies related to data quality on security and data protection

Appropriate Policies and Procedures

4.6.6 The Council will define clearly its key data requirements and assurance arrangements

4.6.7 procedures must exist for all key activities such as major data collection exercises and external returns

4.6.8 All such policies and procedures should be reviewed regularly to consider their impact on data quality and to ensure they reflect any change in need

4.6.9 Departmental managers will ensure that all such policies and procedures are adopted and embedded within working processes and that compliance is achieved

Appropriate Systems and Processes

4.6.10 Clear systems and business processes should exist in which data collection and reporting

4.6.11 Guidelines for all processes supporting key data requirements will exist and be followed consistently

4.6.12 Data should be collected and recorded once only wherever possible without the need for multiple systems

4.6.13 systems should have validation checking facilities to ensure data is complete, consistent and internally validated

Appropriate Security

4.6.14 The Council will have in place appropriate security arrangements to ensure that data is protected from unauthorised access from outside the institution

4.6.15 All Council systems will have security arrangements in place to ensure appropriate levels of access to data by individual staff and students

Appropriate Staff Development

4.6.16 All members of staff accessing, inputting and amending data on Council systems must have the appropriate knowledge, competencies and capacity to carry out the activity and preserve data quality

4.6.17 All policies procedures and guidelines will be communicated effectively to relevant staff, and this will include policies on security and data protection as part of the wider consideration of data quality

Reporting and Presentation of Data

4.7 All management information reports will be clear in what they are representing, bearing in mind the audience for which they are intended, and regular reports should be reviewed to ensure that they reflect any change in need. The review should be balanced with the need for consistency over time so that trends can be recognised and reported.

4.8 External returns will be subject to rigorous validation and verification, submitted on a timely basis and will evidence a full audit trail, including appropriate approval and sign-off as specified by the body to whom the return is submitted, or agreed by the Information Council in the absence of such a recommendation.

New System Developments:

4.9 The identification and consideration of data quality risks and requirements will be undertaken as integral part of system development projects, or programmes, and risk assessed, as appropriate, in conjunction with relevant stakeholders.

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.

5.2 The Data Services Team, in conjunction with the Data Council, will lead the development of Quality Action Plans to implement the quality principles and objectives detailed in this policy.

5.3 The Data Council will be responsible for the implementation of the plan including data cleaning activities, process or system improvements, training and awareness sessions and the ongoing monitoring of quality reports and actions to remedy emerging issues.

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.

Council Leadership Team

6.2 The Council Leadership 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 Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation, including risks around the quality of the Council's data. The Information 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 Council Leadership 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

6.5 The Information Council will be responsible for the approval and on-going monitoring of the Quality Actions Plans.

Data Council

6.6 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:

6.6.1 The development, implementation and review of Quality Action Plans including:

6.6.1.1 Data cleansing

6.6.1.2 Development of guidance and training on Data Quality

6.6.1.3 Implementation of process or system improvements to improve data quality

6.6.2 Monitoring Data Quality Reports and ensuring that actions are undertaken at a service level to remedy issues and avoid reoccurrence

6.6.3 Escalate persist Data Quality issues and action plans to the Information Council.

6.6.4 Production of regular progress report for the Information Council

Information Governance Unit

6.7 The Information Governance Unit, in conjunction with the Data Services Team, will support the implementation of this policy as set out in the IC annual plan.

Data Services Team

6.8 The Data Services team provide specialist data analytical resources and services including data profiling, modelling, visualisation, quality and advanced analytics for the Council.

6.9 Data Services will support implementation of this policy in partnership with the Information and Data Councils as follows:

6.9.1 Development of the Data Warehouse and Data Quality Toolsets

6.9.2 Lead the development of Quality Action Plans in association with the Data Council.

6.9.3 Produce regular systems data quality reports and provide support to the Data Council to identify and implement remedial actions and as required escalate risks through the Councils Risk Management Framework.

6.9.4 Produce a suite of Quality Performance Reports to monitor data quality and progress against the Quality Action Plans for the Data Council and Information Council.

Managers and supervisors

6.10 All managers must:

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

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

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

6.10.4 Support the implementation of approved Quality Action plans and ongoing monitoring of data quality

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

6.11 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

6.12 All staff must:

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

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

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

6.12.4 Assist with the implementation of approved Quality Action Plans and actions to address emerging issues identified by the Data Council.

6.13 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

Council Policy

7.1 Data Quality Policy

7.2 ICT Acceptable Use Policy

7.3 Information Governance Policy

7.4 Information Rights Policy

7.5 Records Management Policy

7.6 Reuse of Pubic Sector Information Policy

Codes, Guidance, Procedures and Strategy

7.7 Employee Code of Conduct

7.8 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 5 – Information Rights Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Kevin Wilbraham, Information Governance Manager
Author	Douglas Stephen, Information Rights Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	18-07-2016	Douglas Stephen	Policy created; incorporates elements of previous FOI Policy
0.2	22-07-2016	Kevin Wilbraham	Policy revised and circulated
0.3	15-08-2016	Kevin Wilbraham	Comments incorporated and further revisions made
0.4	03-09-2016	Kevin Wilbraham	Draft version agreed by Head of Strategy (Interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30/09/2014	Corporate Policy & Strategy	Information Governance Policies	Minute

Information Rights Policy

Policy statement

1.1 This Policy formalises the City of Edinburgh Council's approach to facilitating and promoting our citizen's information rights. In particular, it sets out the Council's commitment to the following principles:

1.1.1 To respect the information rights of individuals in accordance with the principles set out in the Data Protection Act 1998, Freedom of Information (Scotland) Act 2002, Environmental (Scotland) Regulations 2004, INSPIRE (Scotland) Regulations 2009 and the Pupils' Educational Records (Scotland) Regulations 2003.

1.1.2 To advise and assist people in exercising their rights of access to information held by the Council.

1.1.3 To maximise the publication of information through the Council's Publication Scheme, FOI Disclosure Log and other initiatives, including Open Data, and to promote a culture of openness within the Council.

1.1.4 To conduct business in an open, accountable and transparent way to promote trust in how the Council operates.

Scope

2.1 This policy applies to all employees of the Council (including temporary staff) 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. 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 legislation with particular reference to the prompt provision of information where requested by the Council.

2.2 This policy addresses the rights individuals have to request information held by the Council, subject to certain limited conditions and exemptions, exceptions or limitations. This includes:

2.2.1 All recorded information within the definitions contained in the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

2.2.2 Spatial data sets, or spatial data services about the environment or metadata relating to these as defined by the INSPIRE (Scotland) Regulations 2011.

2.2.3 Personal information within the definition contained in the Data Protection Act 1998.

2.2.4 Pupil information as defined under Pupils' Educational Records (Scotland) Regulations 2003.

2.3 This policy also addresses the rights granted to individuals under the Data Protection Act 1998 regarding the processing of their personal data.

Definitions

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

3.2 **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 organisations can use their personal data.

3.3 **Data Subject:** is 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.

3.4 **Exemptions:** Part 2 of the Freedom of Information (Scotland) Act 2002 contains a number of exemptions which, if applicable, means that information covered by a request does not need to be disclosed. Similarly, under the Data Protection Act 1998 exemptions or restrictions may be applied in certain circumstances.

3.5 **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.

3.6 **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.

3.7 **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.

3.8 **Parent:** parents, guardians, individuals who hold parental responsibilities and individuals who have care of a child (e.g. a foster parent or another relative).

3.9 **Personal data (or information):** 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.

3.10 **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.

3.11 **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.

3.12 **Senior Information Risk Owner**: the Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information rights.

3.13 **Sensitive personal data:** requires a higher level of consideration. Information will be considered 'sensitive personal data' if it relates to a person's: racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, and criminal offences or alleged criminal activity (including any criminal proceedings).

3.14 **Subject Access Request (SAR) -** the right granted to an individual by the Data Protection Act 1998 to request a copy of personal information held about them.

3.15 **UK Information Commissioner -** is the independent regulator responsible for ensuring all organisations comply with the Data Protection Act. Organisations are required to notify the ICO of how they process personal data and if they breach the Act. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, impose large fines (up to £500,000), and bring a criminal case against an organisation. Further information about data protection is available on the ICO website at www.ico.org.uk.

Policy content

Dealing with Requests

4.1 The Council has statutory obligations around access to its information. It will comply with these as follows:

4.1.1 Providing a general right of access to its recorded information, excluding environmental information and personal information, under the Freedom of Information (Scotland) Act 2002.

4.1.2 Providing access to its recorded environmental information under the Environmental Information (Scotland) Regulations 2004. These concern matters such as air, water, soil, landscaping, natural sites, biodiversity, human health and safety, and decisions and activities affecting these issues.

4.1.3 Providing access to any of its spatial datasets or spatial data services about the environment, with appropriate metadata, under the INSPIRE (Scotland) Regulations 2009.

4.2 The Council will also meet its statutory obligations under Data Protection Act1998, by supporting individuals in understanding what information is held about them and providing them with a copy of that information, where appropriate. This is known as a 'subject access request' (SAR).

4.3 The Council will also meet its obligations under the Education (Pupil Records) (Scotland) Regulations, 2003, and give parents access to their child's educational records.

4.4 In all of these statutory obligations, the Council has the right and duty to apply certain limitations and exemptions to protect legitimate interests. In particular, it will not provide personal data of third parties without their consent, vital interest or a statutory basis to do so.

4.5 All responses to requests for information will be agreed by a Senior Manager (Tier 3) within the relevant service before they are released.

4.6 The Council will treat any individual request for personal data that has already been sent or disclosed to that individual as a 'business as usual' request and send replacement copies, subject to being satisfied of the individual's identity and right to receive the information.

Request timescales

4.7 The Council will respond to all requests promptly following receipt of a valid request, and will respond within the statutory timescales, as set out below.

4.7.1 Freedom of Information (Scotland) Act 2002: 20 working days

4.7.2 Environmental Information (Scotland) Regulations: 20 working days

4.7.3 INSPIRE (Scotland) Regulations 2009: 20 working days

4.7.4 Data Protection Act 1998: 40 calendar days

4.7.5 Pupils' Educational Records (Scotland) Regulations 2003: 15 school days

4.8 The Council will notify any requestor where a response is likely to be late and will provide a new estimated response date along with advice on their statutory rights.

4.9 Under the Environmental Information (Scotland) Regulations, 2004, the Council can extend the timescale for responding to a request for a further 20 working days, in certain and limited circumstances. The requestor will be notified if the Council does intend to extend the timescale for response and the reason why.

Publishing information

4.10 The Council will proactively publish information to promote and facilitate a culture of openness and transparency. In particular, it will:

4.10.1 Maintain an up to date publication scheme, as required under the Freedom of Information (Scotland) Act 2002, detailing what information the Council routinely makes publicly available.

4.10.2 Identify data which can be shared and used publicly through the Council's Open Data Strategy.

4.10.3 Maintain a publicly available disclosure log which records all requests for information received, and shows the responses issued in relation to those requests.

Withholding and redacting information

4.11 Where the Council seeks to rely on any exemption, exception, condition or limitation for withholding information, it will explain, in detail to the requestor, why this applies to the information requested.

4.12 Similarly, the Council will explain to a requestor why information has been redacted or extracted in order to meet conflicting statutory obligations to both provide access and protect the legitimate interests of third parties.

4.13 The Council will not routinely redact the names of Council officials from information produced in the course of their work, but reserves the right to do so in specific circumstances.

Charging for requests

4.14 The Council will not charge for information provided in the Council's Publication Scheme, unless otherwise stated. There may be a charge for printing and postage.

4.15 The Council will charge requests made under FOI(S)A , EIRs and INSPIRE Regulations where it is appropriate to do so. These charges will be based on statutory guidance and will be published on the Council's website.

4.16 The Council does not routinely charge for subject access requests or requests to view pupil educational records, but reserves the right to do so in line with statutory guidance.

Reviewing requests

4.17 The Council will meet its statutory obligations in providing a process to review its decisions and performance in relation to information request under information rights legislation.

4.18 The Council has 20 working days to respond to such requests but will inform applicants where this may be late.

4.19 The Council commits to supporting the Scottish Information Commissioner, when investigating complaints made against it, and will comply with any decision notices issued by the Commissioner.

4.20 While there is no statutory requirement for the Council to review any concerns raised in relation to the SAR process, the Council will review any such requests for review and respond within 20 working days. The Council does not seek to affect the statutory rights of individuals to notify the UK Information Commissioner's Office if they are unhappy with how the Council has acted.

4.21 The Council will review any concerns raised in relation to the provision of pupil information under the Pupils' Educational Records (Scotland) Regulations 2003 and respond within 20 working days.

Rectification, blocking, erasure and destruction of personal data

4.22 The Council will meet its obligations in relation to the accuracy of personal data under the Data Protection Act 1998 and the Pupils' Educational Records (Scotland) Regulations 2003 by considering and responding to requests made in writing by a data subject or parent to have any factually inaccurate personal data corrected, blocked, erased or destroyed.

4.23 The Council will not alter its records if a data subject or parent disagrees with a recorded professional opinion about them or their child. Where there is disagreement, the Council will notify the data subject or parent and set out the reasons for the decision.

Distress and automated decision making

4.24 Under the Data Protection Act, 1998 alone, there are two further types of requests the Council will consider. These are:

4.24.1 Requests made in writing from a data subject to stop using their personal data where they believe that use is causing them substantial damage or distress.

4.24.2 Requests made in writing from a data subject that any decision that has a significant effect on them is not based solely on automated decision making methods.

4.25 The Council will respond in writing to these notices within 21 days.

Implementation

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

5.2 Key measurements of successful implementation of this policy will be:

5.2.1 Meeting statutory deadlines when responding to requests

5.2.2 Managing the review processes to address concerns without regulator involvement

5.2.3 Operating a model of continuous review and improvement when responding to requests.

5.3 Performance will be routinely reported to the Information Council, Council Leadership Team and other senior management teams, where appropriate

5.4 Council staff will be given awareness, induction and refresher training on information rights legislation.

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 access legislation detailed in this policy.

Council Leadership Team

6.2 The Council Leadership Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate and locality applies relevant information governance policies and controls, including compliance with information rights legislation.

Information Council

6.3 The Information Council (IC) has delegated responsibility, through the Senior Information Risk Owner and the Council Leadership 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 access legislation and associated codes of practice.

Information Governance Unit

6.4 The Information Governance Unit will:

6.4.1 Act as the first point of contact for all information rights issues affecting the Council

6.4.2 Log, process and respond to all information requests received by the Council (excluding any requests under the Pupils' Educational Records (Scotland) Regulations 2003 which are dealt with directly by the school)

6.4.3 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

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

6.4.5 Support schools and teachers in complying with the Pupils' Educational Records (Scotland) Regulations 2003

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

Information Rights Manager

6.5 The Information Rights Manager is responsible for co-ordinating the work of the Information Rights Team, as well as monitoring the manner and timescales in which requests for information are dealt with.

6.6 The Information Rights Manager reports on compliance with the policy and procedures, and also provides monthly performance reports, as required

6.7 The Information Rights Manager also provides guidance and training and has responsibility for the Council's Publication Scheme.

Review Officer

6.8 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. The Review Officer is part of the Information Compliance Team under the Information Governance Unit.

6.9 The Review Officer also acts as the liaison link with external regulators and provides submissions in relation to any appeals made by applicants.

Managers and supervisors

6.10 All managers and supervisors have a responsibility for enabling effective information governance within their respective service areas and teams. In relation to this policy this includes:

6.10.1 The provision of local and effective arrangements to ensure the timely return of relevant information to the Information Governance Unit. This includes compliance with the Council's Records Management and Managing Personal Data Policies.

6.10.2 Ensuring that staff have received information governance training and are aware of their role and responsibilities in relation to identifying and processing requests for information, and assisting applicants.

Head teachers

6.11 All Head Teachers must ensure effective arrangements are in place to ensure compliance with the provisions of the Pupils' Educational Records (Scotland) Regulations 2003, including:

6.11.1 Acknowledging all parental requests to access educational records

6.11.2 Ensuring that requests are valid (requests must be in a written format; must state the name of the applicant and an address for correspondence; and describe the information being requested).

6.11.3 Making arrangements for parents to visit and view records within 15 school days

6.11.4 Ensuring that only relevant information is made available

Staff

6.12 All Council staff will:

6.12.1 Be aware of that the Council has obligations to identify, support and respond to statutory requests for information under the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, the INSPIRE (Scotland) Regulations 2009, the Data Protection Act 1998.

6.12.2 Be able to identify statutory request for information from business as usual requests

6.12.3 Provide basic advice and assistance to persons making such requests for information

6.12.4 Know to pass any these requests to the Information Governance Unit for logging and processing

6.13 Council staff that are nominated as information rights contacts within their service area are expected to assist the Information Governance Unit in providing information and context in responding to requests.

6.14 Nominated contacts must ensure that any information provided is signed off by a Tier 3 manager prior to this being passed to the Information Governance Unit for responding.

School staff

6.15 All school staff must additionally:

6.15.1 Be aware of the requirements of the Pupils' Educational Records (Scotland) Regulations 2003

6.15.2 Be able to identify any request that falls under Pupils' Educational Records (Scotland) Regulations 2003

6.15.3 Provide advice and assistance to parents making requests for information

6.15.4 Know to pass any information request onto the Head Teacher

Related documents

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 Information Governance Policy

7.4 Managing Personal Data Policy

7.5 Record Management Policy

7.6 Re-use of Public Sector Information Policy

Codes, Guidance, Procedures and Strategy

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

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

Legislation

7.9 Data Protection Act, 1998

7.10 Environmental Information (Scotland) Regulations

7.11 Freedom of Information (Scotland) Act 2002

7.12 The Pupil's Educational Records (Scotland) Regulations

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.

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

Appendix 6 – Information Security Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Neil Dumbleton, Enterprise Architect
	Kevin Wilbraham, Information Governance Manager
Author	Henry Sullivan, Information Asset Manager
	Sarah Hughes-Jones, Information Compliance Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	07-07-2016	Henry Sullivan Sarah Hughes-Jones	Initial draft created and circulated for comment
0.2	29-07-2016	Kevin Wilbraham Henry Sullivan	Revisions made and incorporated
0.3	04-08-2016	Kevin Wilbraham Sarah Hughes-Jones	Further revisions made and incorporated
0.4	22-08-2016	Kevin Wilbraham	Consultation version circulated
0.5	24-08-2016	Henry Sullivan	Revisions in light of ICT Solutions consultation
0.6	03-09-2016	Henry Sullivan	Draft versions agreed with Head of Strategy (Interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute

Information Security Policy

Policy statement

1.1 The Council has statutory responsibilities to make sure that the data and information it creates or receives is kept safe and used appropriately.

1.2 The Council depends on the confidentiality, integrity and availability of its information to such an extent that a serious breach of information security could impact on the Council's ability to deliver a wide range of statutory services.

1.3 The Council also has contractual obligations to ensure sound security if it is to use the Government's Public Services Network (PSN); meet Payment Card Industry Data Security Standards (PCI DSS), or receive or share information with partner agencies under information sharing arrangements.

1.4 In setting out the Council's information security arrangements, this policy confirms the Council's commitment to its citizens, visitors, employees and business partners that Council information and data will be properly protected, valued and secured.

1.5 The Council's information security arrangements are based on the provisions of the ISO/IEC 27000 series (the industry standard for information security) and the development and maintenance of an Information Security Management System (ISMS), consisting of this policy and associated standards and protocols.

1.6 The Council requires that its Directorates, Localities, staff and partners operate and deliver its services in compliance with the ISMS and associated standards.

1.7 Failure to comply with this policy may result in sanctions up to and including dismissal or contract termination, as well as the possible involvement of law enforcement and relevant external regulators.

Scope

2.1 This policy and related protocols, procedures and guidance under the Council's ISMS applies to:

2.1.1 All data and information created, received and managed in the course of Council business.

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

2.1.1 All third parties, contractors and suppliers accessing or handling Council information, equipment, network or systems.

Definitions

3.1 **BS ISO/IEC 27001:2013:** This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation, such as the Council.

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

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

3.4 **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.

3.5 **Information asset owners:** Heads of Service involved in managing a business area(s) with responsibility for the information assets within their respective business area(s).

3.6 **The Information Council (IC)**: has delegated responsibility, through the SIRO and the Council Leadership 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.

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

3.8 **Information Security Management System**: preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to internal and external stakeholders that risks are adequately managed.

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

3.10 **Organisational controls**: are measures that instruct and define responsibilities and expected behaviours and practices in terms of information security (e.g. policies, procedures, guidance)

3.11 **Privacy impact assessment**: a risk management method 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.

3.12 **Security impact assessment**: ensures that necessary security controls are integrated into the design and implementation of a project.

3.13 **Senior Information Risk Owner**: the Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation.

3.14 **Technical controls**: are measures that limit and define access and action via network and system configuration in terms of information security (e.g. account management, back up cycles, encryption and firewalls)

Policy content

Strategic approach

4.1 The Council's strategic approach to information security is based on:

4.1.1 The continued development and implementation of an information security strand within the Council's Information Governance Framework.

4.1.2 The alignment of all elements of information security with ISO 27000 (Information Security Management), which is the industry standard for information security and HMG Security Policy Framework

4.1.3 A documented Information Security Management System (ISMS) which details the Council's information security management arrangements and the application of control measures in detail.

4.1.4 The regular review of the ISMS to identify improvements, and to ensure on-going maintenance and implementation of the system.

4.1.5 The continuing availability of specialist information governance/security advice to support the implementation process for information security, and the other areas within the Information Governance Framework.

4.2 In line with the requirements of the Data Protection Act of 1998, the Council has both organisational and technical measures to secure its information. The development, implementation and assurance of these measures are divided between ICT Solutions (Technical) and the Information Governance Unit (Organisational).

Organisation of the Information Security Management System

4.3 The Council's information security management system will consist of protocols, procedures and guidance, all underpinned by this policy.

4.4 This management system will conform to the ISO 27001 standard and will cover the following areas of control:

4.4.1 Human Resources Security and Supplier Management

4.4.2 Information Asset Management

4.4.3 Access Management

4.4.4 Cryptography

4.4.5 Physical and Environmental Security

4.4.6 Business & ICT Operations Security

4.4.7 Protective Marking and Information Handling

4.4.8 Mobile Devices and Removable Media Management

4.4.9 Business Continuity Management

4.5 Each area of control within the management system will have a protocol that outlines compliance requirements. Protocols will be supported by procedures and additional guidance.

4.6 The Council requires that its Directorates, Localities, staff and partners operate and deliver its services in compliance with these standards.

4.7 The Head of ICT Solutions and the Head of Strategy and Insight are the owners of this management system and are responsible for its implementation, maintenance and performance.

4.8 Change control and oversight of process and documentation within the management system will be the responsibility of the Information Council and supported by the Information Governance Unit and ICT Solutions.

4.8.1 Final versions of all documentation of the management system will be maintained by the Information Governance Unit.

4.9 Delivery of the information security management system will be carried out in partnership between the Council and its ICT Provider, CGI Ltd.

4.9.1 The relevant ICT roles and responsibilities and management structure within CGI have been identified in the Security Management Plan arising from Schedule 2.4 of the Council's IT Procurement Contract.

Monitoring of the Information Security Management System

4.10 The Information Council will routinely review the management system's performance to ensure that it meets the Council's statutory and business requirements and its overall strategic objectives.

4.11 The management system will also be reviewed in response to significant incidents or changes to legislation or regulation.

4.12 To support this, the management system will be monitored for effectiveness and non-compliance by an Information Security subgroup of the Information Council made up of the following Council service areas:

4.12.1 ICT Solutions

4.12.2 Information Governance Unit

4.12.3 Facilities Management

4.12.4 Human Resources

4.13 This group will produce reports for the Information Council and SIRO (as appropriate), including:

4.13.1 An annual report detailing the system's effectiveness, resourcing, changes and risks

4.13.2 Quarterly reports detailing security incidents

Communicating the Information Security Management System

4.14 The management system will be broadly communicated to staff and partners through the Council's annual information governance communications plan.

4.15 Communications around specific incidents or threats will be managed by ICT Solutions and CGI (IT incidents and threats) and the Information Governance Unit (organisational incidents and threats), with coordination from the information security subgroup and assistance from Council's Communications service as required.

Risk assessment & management process

4.16 Information security will be risk assessed, documented, managed and mitigated within the Council's wider Risk Management Framework, with regular reporting to the relevant Council risk committees.

4.17 ICT Solutions and the Information Governance Unit will monitor and support managers in identifying, evaluating and mitigating information security risks.

4.18 They will also undertake periodic audits and risk assessments in their own right, reporting to managers and information asset owners as appropriate.

4.19 Identified information security risks can be escalated to the SIRO and be reviewed and managed through the IC if required by the SIRO.

Incident management

4.20 Information security breaches must be reported via the Council's Information Security Incident Management Procedure as soon as possible by the individuals who have caused or discovered the breach.

4.21 While it is appropriate for staff to initially report an incident to their manager where they are available, this must then be reported according to the Information Security Incident Management Procedure as quickly as possible.

4.22 While individual incidents will be handled by the most relevant Council service area, the Information Security subgroup will coordinate and monitor all Council information security breaches.

Information Security in Project Management

4.23 Council projects that involve the handling and sharing of information are covered under the Council's information security arrangements.

4.24 These projects will require a Security Impact Assessment to be undertaken by the relevant project manager or officer with the support of ICT Solutions and the Information Governance Unit, as appropriate.

4.25 Council projects that impact on the privacy of individuals will also require a privacy impact assessment to identify and document appropriate governance controls required to manage the privacy risks associated with new or changed processes that involve personal data.

Training

4.26 This policy and associated protocols will underpin all information security training, both mandatory and refresher training. Training will be supported by further detailed guidance on the Council's intranet.

Implementation

5.1 Implementation of this policy will be undertaken through the continued development, roll out and maintenance of a Council-wide information security management system.

5.2 The information security management system will itself be implemented and continuously improved by the member service areas of the Information Security subgroup through the information security work stream of the Information Council's annual plan.

5.3 Progress and performance will be monitored by the Information Council and reported to the SIRO as appropriate.

5.4 The protocols and guidance of the management system will need to be implemented by managers into business processes and other local documentation. The Information Security Team and Information Governance Unit will support this process, as required.

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 Council's Information Security Management System.

Council Leadership Team

6.2 The Council Leadership Team has overall responsibility for Information Governance. This involves providing high-level support to ensure that directorates and localities apply relevant information governance policies and

controls, including compliance with the Council's Information Security Management System.

Senior Information Risk Owner

6.3 The Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation, including technical and organisational risks around information security.

Deputy Senior Information Risk Owner

6.4 The Information Governance Manager deputises for the SIRO as required and ensures that the Information Governance Framework is compliant with the Council's overall approach to corporate governance.

Information Asset Owners

6.5 Heads of Service are nominated information asset owners with overall responsibility for identifying and addressing any information risks relating to the information assets within their areas, including technical and organisational risks around information security.

Information Council

6.6 The Information Council has delegated responsibility, through the SIRO and the Council Leadership 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 Council's Information Security Management System.

ICT Security Manager - CEC

6.7 The Council's ICT Security Manager is part of ICT Solutions and is the operational lead on technical IT risks and is responsible for overseeing and implementing appropriate controls, in line with best practice, compliance frameworks and this policy. The Information Security service works closely with the Information Governance Unit and the ICT partner to ensure that information governance policies, standards, rules and assurance are applied and assured.

ICT Security Manager - CGI

6.8 CGI's IT Security Manager provide an independent view of IT security across the City of Edinburgh Council ICT Transformation Environment and co-ordinates operational security activities across the various CGI provided programmes and

services in accordance with Information Security Management System and associated plans.

Information Compliance Manager

6.9 The Council's Information Compliance Manager is the operational lead on organisational risks around information security. They are responsible for:

6.9.1 Coordinating and implementing appropriate organisational controls and measures, in line with best practice, compliance frameworks and this policy, and in conjunction with Facilities Management, ICT Solutions and Human Resources.

6.9.2 Assessing and reporting on those controls in line with the Council's Information Security Management System.

6.9.3 Receiving and managing relevant breach and incident reporting and ensure remedial actions have been undertaken and completed, in conjunction with ICT Security.

Facilities Management

6.10 Facilities Management will undertake the routine operation of physical security controls within the Council's estate.

Human Resources

6.11 Human Resources will monitor and provide assurance on organisational security controls in relation to staffing issues.

Managers and supervisors

6.12 Managers and supervisors have a number of responsibilities in relation to information security, and information governance more generally. These are set out in the protocols that form part of the Council's Information Security Management System and the Council's Information Governance Framework. These must be followed at all times.

6.13 In particular, managers and supervisors are responsible for ensuring that all permanent and temporary staff, contractors, partners, suppliers and customers of the Council who have access to Council Information Systems, or information used for council purposes have read and understood this policy (including associated protocols and guidance), and undertaken mandatory training in information governance and information security.

All staff

6.14 Information security is the responsibility of all staff. Individuals must ensure that they have read and understood this policy (including associated protocols and

guidance), and undertaken mandatory training in information governance and information security.

Related documents

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 ICT Acceptable Use Policy

7.4 Information Governance Policy

7.5 Information Rights Policy

7.6 Managing Personal Data Policy

7.7 Records Management Policy

Codes, Guidance, Procedures and Strategy

7.8 Employee Code of Conduct

7.9 In addition to the above there will be a suite of protocols, procedures and guidance on information security developed and published as part of the Council's Information Security Management System

Legislation

7.10 Computer Misuse Act, 1990

Standards

7.11 *ISO/IEC 27000 series – Information technology — Security techniques — Information security management systems*

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 principles of information security are underpinned by legislation, and the consequences of a serious breach of information security are severe.

10.2 The risks of not implementing this policy include:

10.2.1 Distress or harm to individuals or organisations.

10.2.2 Reputational damage to the Council.

10.2.3 Financial loss or monetary penalty imposed.

10.2.4 Detrimental impact on Council business and service delivery.

10.2.5 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 7 – Managing Personal Data Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Kevin Wilbraham, Information Governance Manager
Author	Sarah Hughes-Jones, Information Compliance Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	06-07-2016	Sarah Hughes-Jones	Draft policy created; incorporates elements of previous Data Protection Policy
0.2	21-08-2016	Kevin Wilbraham	Minor comments incorporated; draft circulated
0.3	23-08-2016	Kevin Wilbraham	Further comments incorporated
0.4	26-08-2016	Kevin Wilbraham	Reformatting and updates around guidance
0.5	03-09-2016	Kevin Wilbraham	Draft version agreed with Head of Strategy (interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30/09/2014	Corporate Policy & Strategy	Information Governance Policies	Minute

Managing Personal Data Policy

Policy statement

1.1 This policy sets out and formalises the City of Edinburgh Council's (the Council) approach to managing personal data in accordance with the requirements of the Data Protection Act 1998, and in preparation for the General Data Protection Regulation.

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 (hardcopy and electronic).

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

3.2 **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.

3.3 **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 organisations can use their personal data.

3.4 **Data Subject** – is 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.

3.5 **Edinburgh Integrated Joint Board (EIJB)** – is responsible for delivering the Integration Scheme for the integration of adult health and social care. This is a joint enterprise between the Council, NHS Lothian, and the EIJB constituted under the Public Bodies (Joint Working)(Scotland) Act 2014.

3.6 **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 a data controller must take to achieve compliance. A data controller can lodge an appeal against the Notice to the Information Tribunal. It is a criminal offence for a data controller to fail to comply with a valid Enforcement Notice.

3.7 **European Economic Area** – includes member states of the European Union and three of the member states of the European Free Trade Association (Iceland, Liechtenstein and Norway).

3.8 **General Data Protection Regulation (GDPR)** – is the new data protection regulation which will come into force in May 2018. It builds upon, and strengthens, the compliance regime provided by the Data Protection Act 1998.

3.9 **Information Commissioner -** is the independent regulator responsible for ensuring all organisations comply with the Data Protection Act. Organisations are required to notify the ICO of how they process personal data and if they breach the Act. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, impose large fines (up to £500,000), and bring a criminal case against an organisation. Further information about data protection is available on the ICO website at www.ico.org.uk.

3.10 **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.

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

3.12 **Information (or data) Sharing** – ensures that Council information is shared in a compliant, controlled and transparent manner.

3.13 **Notification** – is the process by which organisations notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. The Information Commissioner uses this information to maintain a Register of Data Controllers which it publishes on its website.

3.14 **Personal data (or information)** – 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.

3.15 **Privacy Impact Assessment** – is a risk management tool that reduces the risks of harm to individuals through the misuse of their personal information. It assists in designing appropriate processes for handling personal data. It is used when projects, or changes to service activities, or new ICT impact on the privacy of individuals

3.16 **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.

3.17 **Safe Harbour** – a set of security arrangements designed to ensure that personal data held outside the European Economic Area receives the same level of security as personal data held within it.

3.18 **Sensitive personal data –** requires a higher level of consideration. Information will be considered 'sensitive personal data' if it relates to a person's: racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, and criminal offences or alleged criminal activity (including any criminal proceedings).

3.19 **Subject Access Request (SAR) -** the right granted to an individual by the Data Protection Act 1998 to request a copy of personal information held about them.

Policy content

Data Protection Principles

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.

4.2 There are eight data protection principles that govern how organisations manage personal data. They are:

4.2.1 Personal data shall be processed fairly and lawfully.

4.2.2 Personal data shall be obtained for one or more lawful purposes, and not processed in a manner incompatible with that purpose.

4.2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.2.4 Personal data shall be accurate and, where necessary, kept up to date.

4.2.5 Personal data processed for any other purpose or purposes shall not be kept for any longer than is necessary for that purpose or purposes.

4.2.6 Personal data shall be processed in accordance with the rights of the data subjects (Subject Access)

4.2.7 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.

4.2.8 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

Designing or revising processes which collect and use personal data

4.3 The Council regularly collects and processes personal data from individuals who receive services or have a relationship with the Council (e.g. suppliers, employees). However, the Council will only obtain, use and retain personal information that it actually needs to fulfil its business and operational requirements.

4.4 A Privacy Impact Assessment (PIA) will be completed when processes or services that involve personal data are designed or revised. The PIA will identify and document appropriate governance controls required to manage the privacy risks associated with the process.

4.5 Specifically, a PIA must be carried out by service areas when:

4.5.1 Council projects or programmes are undertaken

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

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

4.6 Completed PIAs will be registered with the Information Governance Unit.

Informing data subjects & Fair processing

4.7 When collecting personal data, the Council will inform data subjects about why their personal data is required and how it will be used and retained. It will also explain whether the personal data will be shared. This is called a Fair Processing Notice or Privacy Statement.

4.8 Appropriate fair processing information will be provided at the time personal data is collected from data subjects, or when the Council first contacts the data subject in relation to the personal data they have provided.

4.9 It is recognised that in order 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. In such cases, data subjects will be advised if their personal data is to be used in a new way.

4.10 Fair processing information must be approved by the Information Governance Unit and documented within the relevant PIA.

Sharing Personal Data with other organisations

4.11 The Council works with other organisations to provide services. The sharing of personal data between the Council and third parties is subject to formal information sharing protocols. These set out overarching common rules adopted by the Council and its partners with whom it wishes to share data.

4.12 Details of each data sharing process are documented in information 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.

4.13 All new data sharing protocols and agreements must be assured by the Information Council Data Sharing Sub-Group before they are signed/ used.

Disclosing Personal Data

4.14 There are many instances where it will be fair and reasonable to disclose personal data with (and without) the consent of the individual. All requests for personal data and disclosures must be documented.

4.15 Information may be shared through partnership arrangements where there is a data sharing agreement in place or where the individual has authorised disclosure through a mandate.

4.16 When disclosing personal data, the Council will only disclose personal data that is necessary for the stated purpose.

4.17 Data subjects can request access to their own personal data; this is known as a Subject Access Request (SAR). For information about SARs, and other rights of access to information, see the Information Rights Policy.

Disclosure of personal data to Elected Members.

4.18 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.

Disclosure of personal data relating to crime, or required by law

4.19 Section 29 of the Act allows the Council to consider disclosing personal data for the purpose of prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of taxes or duties.

4.20 Section 35 of the Act allows the Council to disclose personal data if it is required for legal proceedings.

4.21 Each request is considered on a case by case basis and must be forwarded to the Information Governance Unit for processing and response.

Unauthorised Disclosure

4.22 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 to knowingly obtain or disclose personal data without the consent of the data controller (the City of Edinburgh Council).

Training

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

Security

4.24 The Council will ensure that appropriate controls are in place to keep personal data secure at all times. This will include ensuring appropriate 'safe harbour' arrangements are made should personal data need to be transferred outside of the European Economic Area.

4.25 The Council's policies on Information Security, including ICT Acceptable Use, Home Working, and the Guidance Note on Protecting Personal Data, must be followed at all times. Particular care should be given to the display and transportation of personal data to ensure that unauthorised access or disclosure is not made whether by accident or design.

Reporting and Managing Data Protection Breaches

4.26 A Data Protection Breach can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, files containing personal data). They can also occur through the unauthorised use or accidental disclosure of personal data by employees, or deliberate attacks on Council systems.

4.27 All Data Protection Breaches must be reported to the Information Governance Unit in accordance with the Council's Data Protection 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.

Data Processors

4.28 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 is the 'data processor' who processes the data on behalf of the Council.

4.29 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.

4.30 Legal services must be consulted before engaging contractors or consultants who process personal data.

Records Management

4.31 All personal data must be held, retained and reviewed in accordance with the Council's Records Management Policy and agreed retention schedules.

Notification

4.32 The Council is required to notify the Information Commissioner about the types of personal data it collects and processes. It is a criminal offence not to notify the Information Commissioner if there is a requirement to do so, or to fail to maintain an up to date notification.

4.33 Elected Members must also notify the Information Commissioner of any processing of personal data they carry out in relation to their constituents or surgeries.

4.34 The Information Governance Unit is responsible for co-ordinating the renewal of the Council's and Elected Members' notification each year.

4.35 All notifications are recorded on the UK Data Protection Register which is available on the Commissioner's website.

Information Asset Register

4.36 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.

Integrated Services under the Edinburgh Integrated Joint Board (EIJB)

4.37 Where personal data is processed for the purpose of delivering an integrated service under the Integration Scheme of the Edinburgh Integration Joint Board (EIJB), the Council, NHS Lothian and EIJB are all Joint Data Controllers in respect of that data processing.

4.38 There is a formal Memorandum of Understanding between the Council, NHS Lothian, and the Edinburgh Integrated Joint Board which sets out how our Joint Data Controller status is managed and services delivered.

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 their constituency work. (See Notification)

Council Leadership Team

6.3 The Council Leadership 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 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 Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership

Team with specific responsibility for information risk and mitigation, ensuring that information threats and breaches are identified, assessed and effectively managed.

Information Governance Manager

6.5 The Information 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 Council Leadership 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. This includes the review of Information Sharing Agreements and monitoring performance against statutory timescales.

Information Governance Unit

6.7 The Information Governance Unit is part of Strategy and Insight 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 the 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 raise awareness through regular communications

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 data is complex (e.g. multi-agency working);

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

6.7.12 Carry out information governance assessments;

6.7.13 Record and maintain the Council's register of information sharing agreements; and

6.7.14 Record and maintain the Council's register of Privacy Impact 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, and 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 to 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 ongoing compliance with this policy and associate 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.

Staff

6.9 All staff have 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 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

Policy

7.1 Data Quality Policy

7.2 ICT Acceptable Use Policy

7.3 Information Governance Policy

7.4 Information Rights Policy

7.5 Information Security Policy

7.6 Record Management Policy

Codes, Guidance, Procedures and Strategy

7.7 Employee Code of Conduct

7.8 Open Data Strategy

7.9 Data Breach Procedure

7.10 Privacy Impact Assessment guidance

7.11 Information sharing guidance

Legislation

7.12 Data Protection Act, 1998

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.

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 is likely to rise considerably subject to the rules set out in domestic legislation following the adoption of the General Data Protection Regulation.

10.2 Individuals may take action against the Council through the Court for any misuse of their personal data. 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 serious reputational impact to the Council.

10.6 Mishandling of personal information may have serious implication 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 the Council committee annually, in line with the Council's Policy Framework.

Appendix 8 – Records Management Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	Kevin Wilbraham, Information Governance Manager
Author	Henry Sullivan, Information Asset Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
1.0	30-09-2014	Henry Sullivan	Version approved by Corporate Policy & Strategy Committee as part of Information Governance Policy Suite
1.1	18-01-2016	Henry Sullivan	Updates for ICO Audit – first draft
1.2	06-07-2016	Henry Sullivan	Updates post Transformation
1.3	25-08-2016	Henry Sullivan	Updated template and link to Data Quality
1.4	03-09-2016	Henry Sullivan	Draft version agreed with Head of Strategy (interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30/09/2014	Corporate Policy & Strategy	Information Governance Policies	Minute

Records Management Policy

Policy statement

1.1 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.

1.2 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.

1.3 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.

1.4 This policy:

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

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

1.4.3 defines records management responsibilities throughout the Council;

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

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

Scope

2.1 This policy applies to:

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

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

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

3.5 **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.

3.6 **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).

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

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

3.9 **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.

3.10 **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.

3.11 **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.

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

3.13 **Record 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;

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

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

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

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

3.14 **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.

Creation

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

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

4.1.3 Council records must be adequate for the Council business they support and based on good quality data, in accordance with the Council's Data Quality Policy.

4.1.4 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.

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

Storage

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

4.1.7 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.

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

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

Management

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

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

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

4.1.13 Council records must not be distributed or copied unnecessarily.

Disposal

4.1.14 No Council record may be destroyed without appropriate authorisation and due regard to both legal obligations and the Council's Retention Schedule.

4.1.15 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.

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

Transfer to Archive

4.2 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.

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

4.4 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.

Records Management Manuals

4.5 Every Council business unit will have at least one Records Management manual that documents the administrative procedures around its business activities, dictating who, when and how records are to be created, stored, managed and disposed or transferred.

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

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

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

4.9 The Council has a Records Management Plan approved by the Keeper of the Records of Scotland (see the published version on the Council's website) and commits to annually reviewing it, as per statutory requirements set out in the Public Records Scotland Act, 2011.

4.10 The Chief Executive of the Council is the senior officer responsible for the Plan. The Information Asset Manager is the Council officer operationally responsible for the Plan.

4.11 The Records Management Plan is maintained and reported on by the Council's Information Governance Unit in conjunction with other relevant officers and overseen by the Information Council.

4.12 An update of changes and improvements to the Council's records management arrangements under the Plan will be made annually by the Council to the Keeper of the Records of Scotland.

4.13 Each new Records Management Plan requested by the Keeper of the Records of Scotland will be approved by the Council Leadership Team and signed off by the Chief Executive before being submitted for the Keeper's approval.

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 Schedule

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

5.2.5 Roll out of the Council's Enterprise Content Management solution

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.

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 the senior officer 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 are up to date, authorised, comprehensive and relevant record retention rules for their directorate within the Council's Retention Schedule

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 **Head of Strategy and Insight** as the **Senior Information Risk Owner** (SIRO) has the delegated responsibility to authorise, in conjunction with each Director, record retention rules that define how long records should be retained and what should happen to them subsequently. The Information Governance Manager is the Deputy SIRO and will act on the SIRO'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 and maintained within records management manuals

6.5.3 ensure that records under their management are retained and disposed of according to the Council's record retention rules – irrespective of format (e.g. electronic / paper) or location (e.g. local storage or at the Records Centre)

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

6.5.5 identify those Council records that are vital to the continuation of Council business and detail them within the Council's business continuity arrangements and their own local records management manuals

6.5.6 consult the Information Governance Unit and their Directorate Records Officer when changes to the Council's record retention rules or File Plan are needed to be made

6.5.7 ensure that records sent to the Council's Records Centre are appropriately listed, with relevant record retention rules given

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

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 the record retention rules that fall within their Directorate.

6.9.3 monitor and authorise records management arrangements within relevant contracts of their directorate.

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

6.10 The **Council Information Asset Manager** is part of the **Information Governance Unit** within the Strategy and Insight division of the Chief Executive's Office. The position has responsibility for the day to day operation and delivery of the Council's Records Management Plan. In relation to records management this officer 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 Schedule;

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

6.10.7 support and contribute to information governance assessments around Council records.

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

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 ICT Acceptable Use Policy

7.4 Information Governance Policy

7.5 Information Rights Policy

7.6 Managing Personal Data Policy

7.7 Re-use of Public Sector Information Policy

Codes, Guidance, Procedures and Strategy

7.8 Code of Practice on Records Management issued under Section 61 of the Freedom of Information (Scotland) Act, 2002

7.9 Council Archives Transfer Procedure

7.10 Council Records Retention Procedure

7.11 Employee Code of Conduct

7.12 Open Data Strategy

7.13 Records Management Manual guidance and workbook

Legislation

7.10 Public Records Scotland Act, 2011

Standards

7.11 *ISO 30300 and 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.

7.12 *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 and the Council's own Records Management Plan.

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 and 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

11.1 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.

Appendix 9 – Re-use of Public Sector Information Policy

Implementation date:

Control schedule

Approved by	
Approval date	
Senior Responsible Officer	
Author	Kevin Wilbraham, Information Governance Manager
Scheduled for review	

Version control

Version	Date	Author	Comment
0.1	21.08.16	Kevin Wilbraham	Policy created and first draft circulated
0.2	28-08-2016	Kevin Wilbraham	Comments incorporated
0.3	03-09-2016	Kevin Wilbraham	Draft version agreed by Head of Strategy (interim)

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute

Re-use of Public Sector Information Policy

Policy statement

1.1 The Re-use of Public Sector Information Regulations 2015 ("the Regulations") provides a legal framework to encourage the re-use of public sector information. This policy formalises and sets out the City of Edinburgh Council's ("the Council") approach to complying with the Regulations, and reaffirms the Council's commitment to open data.

Scope

2.1 This policy applies to all information (regardless of format) produced, held or disseminated by the Council which relate to the delivery of services and provision of a statutory function. These are defined by the Council's Public Task.

2.2 All Council staff, including temporary staff, contractors, consultants and volunteers that create and manage Council information are covered by this policy, including third parties that carry out a statutory function or service on behalf of the Council.

Definitions

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

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

3.3 **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, and the proactive identification of data sets that can be published on the Council's Open Data Portal.

3.4 **Freedom of information laws**: comprises of the Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009.

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

3.6 **Information asset**: information that is defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

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

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

3.9 **Machine-readable format**: a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure. Information is in a standard computer language (not English text) that can be read automatically by a web browser or computer system (e.g., XML or CSV).

3.10 **Marginal cost**: limited to the cost of collection, production, reproduction, provision and dissemination of information (which for digital or online information may be nil) for most public sector bodies.

3.11 **Metadata**: information that describes or defines other information, includes file descriptions, codebooks, processing details, sample designs, etc

3.12 **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. Public sector information and its metadata should available in open format whenever possible.

3.13 **Public sector information**: information collected, held, produced, reproduced or disseminated by a public sector body while accomplishing its public task.

3.14 **Public task**: what a public sector body does, or produces, holds, collects or provides to fulfil its core role and functions, whether those are statutory or established through custom and practice

3.15 **Publication Scheme**: Details what information the Council routinely makes publicly available. A requirement under the Freedom of Information (Scotland) Act 2002,

3.16 **Re-use**: using information for a purpose other than the initial public task purpose for which the public sector body produced, collected, held or disseminated the information. Re-use can be for either commercial or non-commercial purposes.

Policy content

Legislative context

4.1 The Re-use of Public Sector Information Regulations 2015 (“the Regulations”) provides a legal framework to encourage the re-use of public sector information. It creates a right to apply to re-use information which is held by the Council.

4.2 Under the Regulations, re-use means using public sector information for a purpose different from the one for which it was originally produced, held or disseminated, including commercial and non-commercial purposes. This aligns with the Council’s vision for Open Data and is designed to promote economic opportunities, enhance job creation, and improve the flow of information from the public sector to the citizen.

4.3 The Council's Public Task determines what information produced, collected or held by the Council falls within the scope of the Regulations. The Public Task relates to a public authority's core statutory role, including functions established through custom and practice. The Council's Public Task is set out in the appendix to this policy.

4.4 Under the Regulations, public authorities have to produce an information asset list. This requirement is provided by the Council's Publication Scheme which details the classes of information that the Council routinely makes available.

4.5 The Regulations are concerned with permitting the re-use of information and how it is made available. It is not about accessing information. Access rights are covered by Scotland's freedoms of information laws which provide statutory rights of access to information held by the Council. Obtaining information in this way does not provide an applicant with an automatic right to re-use that information. An application must still be made under the Regulations.

Open Data

4.6 The Council's vision for Open Data is that "data will be open by default, of a high quality, timely, comprehensive and usable by all". To deliver this vision, significant amounts of Council information and data sets are already available for re-use through the Council's Open Data Portal.

4.7 Information already available through the Council's Open Data Portal, unless otherwise indicated, is offered under the Open Government Licence. This means that a re-use application is not required. If the information is not available through Open Data Portal but is part of the Council's Public Task, the council will consider all requests to re-use information under the Regulations.

4.8 All data sets released under the Regulations will be considered for open data publication with a presumption in favour of publication whenever possible.

4.9 Similarly, data sets released under Scotland's freedom of information laws will be considered for open data publication, subject to assessment around copyright and formatting issues.

Dealing with requests

4.10 When making a re-use request, applicants must:

4.10.1 submit their requests in writing,

4.10.2 provide their name and a correspondence address,

4.10.3 specify the information they want to re-use,

4.10.4 state what the purpose they intend to use it for.

4.11 If the information has not been previously disclosed, the request will be treated as a request for information under Scotland's freedom of information laws to determine if the information is exempt. Only when the information is provided will

it become eligible for re-use. At that point the re-use element of the request will become a valid re-use request.

4.12 The Council will respond to re-use requests within 20 working days. This timescale may be extended if the request involves an extensive number of documents or raises complex issues. If the timescale is extended, applicants will be informed before the 20 working day deadline why the response time has been extended, and provided with a date on which to expect a response.

4.13 If Council receives two requests from different applicants, it will not discriminate between them. This means that exclusivity arrangements can only be granted in exceptional circumstances and will be subject to regular review.

Formats

4.14 The Council will make information available for re-use in the format and language in which we hold it. The Council will endeavour, whenever possible, to make information available in a machine readable format with appropriate metadata.

4.15 The Council can refuse re-use requests where valid exceptions apply. These may include:

4.15.1 Information for which the copyright is held by a third-party.

4.15.2 Information that falls outside the scope of the Council's Public Task.

4.15.3 Information that contains personal data.

4.15.4 Information exempt from disclosure under information access legislation such as the Freedom of Information (Scotland) Act 2002.

4.16 The Regulations do not apply to third-party copyright information. Any applicant requesting re-use of such information will be directed to the copyright holder. Where the copyright is jointly held by the Council and a third party, the permission of both bodies must be agreed before re-use is permitted.

4.17 Where requests are refused, the applicant will be advised of the decision and their right to make a formal complaint.

Charging

4.18 The Council can charge marginal costs for allowing the re-use of its information. These are limited to the reproduction, provision and dissemination of documents. There are three exceptions to this:

4.18.1 Where the Council is required to generate revenue to cover a substantial part of the costs relating to our public task.

4.18.2 Where the Council is required to generate revenue from documents to cover a substantial part of our costs.

4.18.3 Where the information is held for the purposes of our libraries, museums or archives.

4.19 While the Council reserves the right to charge, it is committed to providing information at no cost whenever possible. Any costs levied will be based on a reasonable rate of return for the re-use of the requested information. Applicants will be made aware of any costs at the time of their application and their right to make a formal complaint.

Terms and conditions of re-using information

4.20 The Council is committed to being as open and non-restrictive as possible in relation to re-use requests. To achieve this Council will use the Open Government Licence. This arrangement is already used as part of the Council's Open Data arrangements and allows the re-use of public sector information without charge for any purpose, commercial or otherwise, with minimal conditions.

4.21 Other licences may be appropriate in particular situations, including where a charge for re-use is permitted beyond the marginal cost of reproduction, provision, and dissemination of documents.

4.22 Applicants will be made aware of licensing arrangements at the time of their application and their right to make a formal complaint. Applicants are expected to read and understand their responsibilities in relation to any licensing arrangements.

Complaints procedure

4.23 Re-use complaints will be dealt with through the Council's freedom of information review procedures, and a response issued within 20 working days. This timescale may vary depending on the complexity of the matter. Complainants will be informed

4.24 If an applicant is not satisfied with the Council's response to their complaint, they can complain to the UK Information Commissioner. The UK Information Commissioner will confer with the Scottish Information Commissioner (as appropriate) and investigate and assess if the Council has met its obligations under the Regulations.

4.25 Any complaints to the UK Information Commissioner must be in writing, state the nature of the complaint, and include a copy of the Council's decision notice.

Implementation

5.1 This policy will be implemented and monitored through the Information Council's annual plan. The plan will outline key tasks, outcomes, accountabilities and progress.

5.2 Key measurements of successful implementation of this policy will be:

5.2.1 Meeting deadlines when responding to requests

5.2.2 Managing the review processes to address concerns without regulator involvement

5.2.3 Operating a model of continuous review and improvement when responding to requests.

5.3 Performance will be routinely reported to the Information Council, Council Leadership Team and other senior management teams, where appropriate

5.4 Council staff will be given awareness, induction and refresher training on the Regulations.

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 access legislation detailed in this policy.

Elected Members

6.2 All Elected Members will be aware of the Regulations and know to pass any re-use requests to the Information Governance Unit.

Council Leadership Team

6.3 The Corporate Leadership Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate and locality applies relevant information governance policies and controls, including compliance with the Regulations.

Senior Information Risk Owner

6.4 The Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO) within the Chief Executive's Office. The SIRO has delegated authority through the Corporate Leadership Team with specific responsibility for information risk. The SIRO ensures information risks are identified, assessed and effectively managed, including compliance issues concerning the Regulations.

Information Governance Manager

6.5 Accountability for the on-going strategic development of information governance lies with the Information Governance Manager within the Strategy & Insight service area of the Chief Executive's Office. The Information Governance Manager deputises for the SIRO as required.

Digital Innovation Manager

6.6 The Digital Innovation Manager is responsible for the continued development of the Council's Open Data Strategy and Open Data Portal.

Information Council

6.7 The Information Council (IC) has delegated responsibility, through the SIRO and the Corporate Leadership 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 Regulations and the on-going development of open data within the Council.

Information Governance Unit

6.8 The Information Governance Unit will:

6.8.1 Act as the first point of contact for all re-use requests received by the Council.

6.8.2 Log, process and respond to re-use requests received by the Council.

6.8.3 Assess and allocate re-use requests to the relevant service to ask them to identify any relevant, recorded information that they hold which would fulfil the request.

6.8.4 Liaise with services concerning exemption/ charge/ licence condition.

6.8.5 Provide the final decision as to whether any exemption/ charge/ licence condition applies to the re-use request.

Information Rights Manager

6.9 The Information Rights Manager is responsible for:

6.9.1 Co-ordinating the work of the Information Rights Team, including monitoring compliance with re-use requests.

6.9.2 Maintenance of the Council's Publication Scheme

6.9.3 Providing guidance and training in relation to the Regulations

Review Officer

6.10 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. The Review Officer is part of the Information Compliance Team under the Information Governance Unit.

6.11 The review officer also acts as the liaison link with external regulators and provides submissions in relation to any appeals made by applicants.

Managers and supervisors

6.12 All managers and supervisors have a responsibility for enabling effective information governance within their respective service areas and teams. In relation to this policy this includes:

6.12.1 Providing local and effective arrangements to ensure the timely return of relevant information to the Information Governance Unit to fulfil re-use requests.

6.12.2 Pro-actively identifying data sets that can be published on the Council's Open Data Portal.

6.12.3 Ensuring that staff have received information governance training and are aware of their role and responsibilities in relation to identifying and processing re-use requests, including assisting applicants when required.

Staff

6.13 All Council staff must be able to:

6.13.1 Identify any request that falls under the Regulations.

6.13.2 Provide advice and assistance to persons making re-use requests.

6.13.3 Know to pass any re-use requests onto the Information Governance Unit.

6.14 As part of their role and remit, individuals may also be nominated as Data Stewards with operational responsibility for data quality and the proactive identification of data sets that can be published on the Council's Open Data Portal.

Related documents

Council Policy

7.1 Archives Policy

7.2 Data Quality Policy

7.3 Information Governance Policy

7.4 Information Rights Policy

7.5 Information Security Policy

7.6 Managing Personal Data Policy

7.7 Records Management Policy

Codes, Guidance, Procedures and Strategy

7.8 Employee Code of Conduct

7.9 Open Data Strategy

Legislation

7.10 Re-use of Public Sector Information Regulations, 2015

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 reputational damage to the Council, 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 9b – City of Edinburgh Council Statement of Public Task

Statement

This statement sets out the functions carried out by the City of Edinburgh Council that are within our public task under the Re-use of Public Sector Information Regulations 2015 (the Regulations). Re-Use means the use of public sector information for a purpose other than the initial purpose for which it was produced, held, collected or disseminated.

The City of Edinburgh Council's powers are conferred by statute and include:

- **Mandatory powers –** such as providing schooling and social work services
- **Permissive powers –** such as economic development and recreation services
- **Regulatory powers –** such as planning control, trading standards, environmental health and the issue of licences for taxi's and public houses

The City of Edinburgh Council is responsible for the provision of a range of public services within the Edinburgh area. The main services the Council provides, in addition to its regulatory and licensing functions, are:

- Arts
- Culture
- Economic Development
- Education
- Environmental Protection
- Housing and the Build Environment
- Sport
- Libraries
- Parks
- Roads and Transport
- Social Work
- Waste Management

In addition, The Local Government Scotland Act 2003 gives a statutory basis for partnership working between all agencies (such as health boards, benefits agencies, further and higher education institutions) responsible for public service delivery in an area. This partnership approach is called Community Planning. The Council is responsible for initiating, facilitating and maintaining Community Planning within the Edinburgh area.

Information which the Council produces in the delivery of these public tasks is generally available for re-use under the Regulations. However:

- the Regulations do not apply to information that would be exempt from disclosure under information access legislation, e.g., the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004;

- the Regulations do not apply to documents held by schools; and
- the Regulations do not apply to a document where a third party owns certain intellectual property rights in the document.

Details of information that we have already published for re-use can be found on the open data pages of our website and in the Council's Publication Scheme.

Review of public task statement

This statement is regularly reviewed and is due to be considered again in April 2017.

Request for re-use of information

If you wish to apply for access to our information under the Re-use of Public Sector Information Regulations please email the Council's Information Governance Unit at foi@edinburgh.gov.uk, or write to them at:

Information Governance Unit
City of Edinburgh Council
Business Centre 2:1
Waverley Court
4 East Market Street
Edinburgh
EH8 8BG

Queries and complaints

If you have any queries on this public task statement, you can submit them to this email address (add relevant email address in here). If you have a complaint about the City of Edinburgh Council under the Re-use Regulations, you can contact us at legalfoi@edinburgh.gov.uk.

If you remain unhappy with our response, you can make an appeal to the Office of the UK Information Commissioner online at: https://ico.org.uk/concerns/getting, or by post to the address below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Alternatively, you can contact the UK Information Commissioner's office via telephone on 0303 123 1113.