Information Governance Policy

Implementation date: 4 October 2016

Control schedule

Approved by	Corporate Policy and Strategy Committee
Approval date	04/10/2016
Senior Responsible Officer	Jo McStay, Strategy and Insight Senior Manager
Author	Kevin Wilbraham , Information Governance Manager
Scheduled for review	October 2017

Version control

Version	**Date**	**Author**	**Comment**
0.1	05.09.14	Kevin Wilbraham	Circulated for comment; minor changes incorporated
0.2	17.09.14	Kevin Wilbraham	Agreed by Information Council
1.0	30.09.14	Kevin Wilbraham	Agreed by CP&S
1.1	03.08.16	Kevin Wilbraham	Revised to reflect organisational change and audit recommendations; circulated for comment
1.2	01.09.16	Kevin Wilbraham	Changes incorporated from Head of Strategy (Interim)
1.3	03.09.16	Kevin Wilbraham	Revised draft agreed with Head of Strategy (Interim)
2.0	04.10.16	Kevin Wilbraham	Approved by CP&S
2.1	03.08.16	Kevin Wilbraham	Revised to reflect legislative changes

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30/09/2014	Corporate Policy & Strategy	Information_Governance_Policies	Minute
04/10/2016	Corporate Policy & Strategy	Information_Governance_Policies	Minute

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.

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

3.1.2 **Data Protection Officer (DPO):** is responsible for monitoring the Council’s compliance with data protection principles, and providing advice to Senior Management on data protection issues. They are also the key contact between the Council and the ICO. The Council’s DPO is the Information Governance Manager.

3.1.3 **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.

3.1.4 **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**.**

3.1.5 **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.

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

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

3.1.8 **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.

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

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

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

3.1.12 **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.

3.1.13 **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.

3.1.14 **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.

3.1.15 **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)

3.1.16 **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.

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:

4.4.1 Data quality

4.4.2 Information rights

4.4.3 Information security

4.4.4 Records and archives management

4.4.5 Re-use and open data

4.4.6 Managing Personal Data

Policies

4.5 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

4.6 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

4.7 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.

4.8 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

4.9 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

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

4.10.1 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.

4.10.2 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

4.11 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

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

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

4.14 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

4.15 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.

Data Protection Impact Assessments

4.16 Data Protection 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

4.17 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

4.18 The Senior Information Risk Owner will present an information governance report to Committee at regular intervals. The report will outline key issues and risks, and will serve as a base line to evaluate future performance and development.

Annual action plan

4.19 The Council's Senior Information Risk Owner will agree 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

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 ensures that the Information Governance Framework is compliant with the Council's overall approach to corporate governance.

Data Protection Officer

6.5 The Council's Information Governance Manager is the Council's Data Protection Officer (DPO). The DPO is responsible for ensuring that the organisation is compliant with GDPR and the future Data Protection Act 2018. The DPO must also be able to act independently, be adequately resourced, and be able to report directly to senior management to raise concerns.

Information Governance Unit

6.6 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

7.1 Related documents include:

7.1.1 Archives Policy

7.1.2 Data Quality Policy

7.1.3 Re-use of Public Sector Information Policy

7.1.3 ICT Acceptable Use Policy

7.1.4 Information Rights Policy

7.1.5 Information Security Policy

7.1.6 Managing Personal Data Policy

7.1.7 Records Management Policy

7.1.8 Employee Code of Conduct

7.1.9 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.