Information Risk Policy

September 2023

Summary Sheet

Document Information

Protective marking (Official /Official-Sensitive-Personal/Official-Sensitive-Commercial/Official-Sensitive-Confidential)	Official
Ref	IG Policy 4.2
Document purpose	Information Risk Policy
Document status (Draft / Active)	Active
Partners (If applicable)	N/A
Date document came into force	1/11/2014
Date of next review	August 2025
Owner (Service Area)	Sefton Council – Strategic Support
Location of original (Owner job title / contact details)	Data Protection Officer – as above.
Authorised by (Committee/Cabinet)	Information Management Group - November 2023 Audit & Governance Committee - TBC

Document History

Version	Date	Author	Notes on revisions
1.0	November 2014	Ben Heal DPO who revised document purchased from Act Now IG consultancy.	On ICO advice to be taken to full Cabinet for ratification.
2.0	August 2021	Catherine Larkin DPO	Revisions throughout
3.0	September 2023	Catherine Larkin DPO	Update - Risk Appetite Framework

Contents

1 Introduction

This policy sets out a formal information risk management programme in Sefton Council. Responsibility for identifying, reporting, managing and mitigating information risk is specifically allocated as part of this policy.

Sefton Council is required to introduce and embed information risk management into key controls and approval processes of all major business processes and functions.

This policy seeks to ensure that the risks to information are recognised as part of that process. This policy complements Sefton Council's existing Corporate Risk Management Strategy and Policy and does not supersede them.

A copy of the Council's Corporate Risk Policy and Risk Management Handbook can be found at the following link:

http://intranet.smbc.loc/our-council/risk-and-resilience.aspx

The Corporate Risk register identifies, assesses and records any key risks associated with information compliance to ensure that any risk that prevents or compromises the achievement of the Council's aims and objectives are managed and adequately monitored.

2 Purpose

- As far as possible, protect data subjects, Sefton Council and its staff from information risks where the likelihood of occurrence and the consequences are significant;
- Comply with Sefton Council's obligations under the UK General Data Protection Regulation and Data Protection Act 2018, especially the need to put appropriate technical and organisational measures in place to prevent loss, theft or damage to data and to meet the principles of storage limitation, data minimisation and accuracy.
- Provide a risk management framework in which information risks are identified, reviewed and mitigated wherever possible;
- Encourage a sense of local responsibility for the information under individual service control
- Encourage pro-active rather than reactive risk management

3 Definitions

Key definitions are:

Risk: the chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Consequence: the outcome of an event or situation, i.e. a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Likelihood: a qualitative description or synonym for probability or frequency.

Risk Assessment: the overall process of risk analysis and risk evaluation.

Risk Management: the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk Treatment: selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

- Avoid the risk
- Reduce the likelihood of occurrence
- Reduce the consequences of occurrence
- Transfer the risk
- Retain/accept the risk

Risk Management Process: The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

4 Responsibilities for Information Risk

4.1 Chief Executive

The Chief Executive has delegated responsibility for the oversight and implementation of information risk management to the role of Senior Information Risk Owner (SIRO) for Sefton Council.

4.2 SIRO (Senior ICT and Digital Manager)

The SIRO is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for Sefton Council. It is their role to:

- Oversee the development and implementation of this policy and a strategy for implementing the policy
- Take ownership of risk assessment process for information risk including review of risk assessments carried out on Information Assets
- Review and agree action in respect of identified information risks.
- Ensure that the Sefton Council's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure executive management is adequately briefed on information risk issues.

4.3 Information Security leads

The Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO) are responsible for the identification, delivery and management of an information risk management programme to address and manage risks to Sefton Council's Information Assets. The Council's main collective decision-making forum is the Information Management and Governance Executive Group, which is also the 'oversight' group providing direction and guidance across the Council for data protection and information governance activities.

4.4 Information Asset Owners (IAO)

The Information Asset Owner (IAO) is a senior manager within a specific department or service are of the Council. They are a manager who is the nominated owner for one or more identified information assets of the department or service area. Sefton Council's Information Asset Owners will be required to:

- Ensure the confidentiality, integrity, and availability of all information that their system processes and protect against any anticipated threats or hazards to the security or integrity of such information.
- Undertake information risk assessments on all information assets where they have been assigned 'ownership', following guidance from the Information Security lead on assessment method, format, content, and frequency.

Further information can be found on the Intranet at the link below, along with a list of all the current Information Asset Owners and Information Asset Administrators:

http://intranet.smbc.loc/our-council/data-protection-information-handling/information-asset-owners.aspx

4.5 All Staff

Everyone has a role in the effective management of risk, including information risk. All staff must actively participate in the process of information risk management by:

- identifying and reporting potential information risks in their area
- contributing to the implementation of appropriate treatment actions
- handling and sharing information responsibly at all times

All employees and Members are required to undergo mandatory information compliance training as part of their Induction when they start work for the Council and to sit refresher training each year. An assessment must be completed at the end of the training to test staff understanding and includes a minimum pass mark. Staff must also complete feedback questions which are provided to the Information Management and Governance Executive group each month.

5 Information Risk Management Process

5.1 Information Assets

The National Archives (TNA) defines information assets as:

'*An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles'*.

Source: Information Asset Factsheet – The National Archives

It is a key principle of data protection law that personal data should not be retained for longer than is necessary – this is known as the 'storage limitation' principle. However, management of all information assets, not just personal data is vital, so we reduce the risk of holding information, which is irrelevant, excessive, inaccurate or out of date.

Drawing upon the TNA's 'Disposal of records' guide produced in support of the good practice recommendations in the Code of Practice on Records Management issued by the Lord Chancellor under section 46 of the Freedom of Information Act 2000, we are guided to consider the value of our records, in terms or organisational and archival:

Organisational value

Organisational value focuses on the organisation's needs and obligations and on records as information assets. It is about value for accountability, legal or reference purposes and includes protection of the legal and other rights of the organisation and those with whom it deals, and compliance with whatever regulatory framework applies.

Archival value

Archival value has a wider and more long-term focus. Archival value is about value for corporate memory purposes and for historical or cultural purposes. Often the records which need to be kept in the long term because of their organisational value are also the records with archival value.

TNA sets out the following questions to assess whether something is an information asset:

- Does it have a value to the organisation? Will it cost money to re-acquire the information? Would there be legal, reputational or financial repercussions if you could not produce the information on request? Would it have an effect on operational efficiency if you could not access the information easily? Would there be consequences of not having this information? Is there a risk associated with the information?

- Is there a risk of losing the information? A risk that the information is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?

- Does the group of information have a specific content? Do you understand what it is and what it is for? Does it include all the context associated with the information?

- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Information assets come in many shapes and forms. The following list is therefore illustrative. It is generally sensible to group information assets in a logical manner e.g. where they all related to the same information system or business process. Typical assets include, but are not limited to:

- Databases and data files
- Back-up and archive data
- Audit data
- Videos and recordings
- Paper records
- Reports, plans and other strategic documentation
- Financial records
- Applications and System Software
- Data encryption utilities
- Development and Maintenance tools
- Computing hardware including PCs, Laptops, PDAs, communications devices e.g. mobile phones and removable media

All information assets are documented within the Sefton Council's Information Asset Register, together with the details of the 'Information Asset Owner' and risk reviews undertaken or planned. The priority are those assets which contain service user, patient or other personal data, or those which contain confidential or safety-critical data. This should be reviewed by IAOs on an annual basis.

Key aspects to establish are:

- Identification of information types which need protection, e.g. personal data or confidential and to review whether the arrangements are adequate
- Identify with whether there is information/data that can be immediately destroyed e.g. trivial/duplicated/obsolete/the retention date has expired?
- Ensure retention schedules are assigned to the information types
- Identify key corporate information assets and assess whether these are being exploited sufficiently

In assessing the business requirements for our information assets, we may find assets which are no longer required and action should be taken to dispose of them.

Further information on the Council's Risk Management Process and 'Risk Appetite' can be found in the Corporate Risk Policy and Risk Management Handbook. Please see the link below:

[Risk and Resilience (smbc.loc)]

Risk Appetite

Risk appetite can be defined as 'the amount and type of risk that the Council is willing to take in order to meet its strategic objectives. Organisations in general will have different risk appetites depending on their sector, culture and objectives. In practice, there is likely to be a range of appetites which exist for different risks, and these may change over time.

Audit and Governance Committee have also now endorsed a **Risk Appetite Framework** for the Council which sets out the level of risk that members have decided is acceptable for the organisation and gives a framework within which officers can make proposals and take delegated decisions.

Further information on the Risk Appetite Framework (RAF) can be found in Annex C of the Corporate Risk Management Handbook.

5.2 Information Risk Manual records

Information assets have risks associated with them; risks from losing an asset, accidental disclosure, misuse by an individual, corruption of the asset or any number of other issues. By considering these risks we should be able to mitigate against them and form contingency plans. Any such risks should be escalated to appear on departmental or corporate risk registers.

Any loss or theft of a Council owned asset, such as a laptop or mobile phone must be reported immediately to the ICT Service desk.

The majority of information assets held by the Council are held electronically but some manual records still exist within particular service areas of the Council. It is recommended that at least once a year, risk assessments of manual records are conducted.

The frequency and method of such assessments must be undertaken via departmental Information Asset Owners in conjunction with their Assistant Director and findings reported back to the Council's Information Management and Governance Executive. Where manual/paper records are identified during the course of an information audit, these must be documented on the information asset register and a risk assessment form completed.

Information Risk Assessments should be routinely undertaken to include assurance of compliance with legislative and regulatory requirements and other information or records management standards as appropriate. Conducting such assessments will help to improve better change management, improved understanding of information risk and identification of potential savings and efficiencies.

A copy of the risk assessment form is available on the Intranet alongside this policy.

5.3 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing, which are:

- We plan to use systematic and extensive profiling with significant effects.
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

If you are unsure whether you need to conduct a DPIA, consult the Council's DPO. You may also need to consult with individuals and other stakeholders throughout the process.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

It seeks to identify privacy risks for individuals (citizens and staff) and compliance risks for the Council. A DPIA must include the following:

- A description of the nature, scope, context and purposes of the processing
- An assessment of the necessity, proportionality and compliance measures
- The identification of risks to individuals arising from the processing proposed and assessment of the risks
- The measures required to mitigate any identified risks

A DPIA is a key risk management tool, and an important part of integrating 'data protection by design and by default' across the Council. It helps to identify, record and minimise the data protection risks of projects.

Guidance on undertaking a Data Protection Impact Assessment for new or existing systems can be sought from the Council's Data Protection Officer (DPO). If your DPIA identifies a high risk and measures cannot be taken to reduce that risk, the ICO must be consulted. Processing cannot start until the ICO has been consulted.

5.4 Information Incident Reporting

Any incident involving actual or potential breaches of personal data, confidentiality, and Sefton Council's information governance policies must be reported to the Council's DPO and investigated in line with Sefton Council's existing incident reporting procedures. See Data Breach Reporting procedure on the Intranet.

http://intranet.smbc.loc/our-council/data-protection-information-handling/data-breach.aspx

Any incident involving actual or potential breaches of information security on ICT systems must be reported to the Council's Senior Manager ICT and Digital (also the Council's SIRO) and the IT Service Desk.

5.5 Monitoring & Review

The Information Risk Policy will be reviewed on a bi-ennial basis by the Information Management Group Executive.