Scottish Funding Council

Information Management Framework

Contents

Introduction

1. This framework and associated policies and procedures describe how we will manage our corporate information to ensure its best use and to comply with codes of best practice and statutory obligations. The framework has two main elements:

    - Ensuring the security of the information.
    - Managing the complete lifecycle of the information.

Who does this framework apply to?

2. This framework, together with its accompanying policies and procedures, applies to all permanent and temporary employees, contractors, consultants, secondees and others who have access to, create, receive or store any corporate information.

3. SFC owns information created by employees carrying out our business related activities. Individual employees do not own our corporate information; however they do have responsibilities for managing it.

4. Staff will have access to information management training and guidance and we will provide supporting procedures and guidelines for them. We will review our policies regularly to ensure they continue to be relevant.

What does this framework cover?

5. This framework applies to the management of all information, in any format or media, created, received, stored and disposed by us while carrying out our business activities. For the purposes of this framework 'information' will be considered to include any recorded data or records held by SFC.

6. Some examples of corporate information:

    - Electronic (e.g. word processed documents, databases, spreadsheets and web content).
    - Emails and their attachments.
    - Paper based documents (including drafts, hand-written notes and annotated copies).
    - Maps and plans.
    - Photographs and digital images.
    - Audio data.

7. Some examples of information formats used to process and store our data:

   - Voicemail.
   - Mobile phone texts.
   - Laptops and tablets.
   - Faxes.
   - Intranet and internet web pages.
   - Audio and video tapes, disks, and flash drives.
   - Social networking – such as Facebook – and Twitter feeds.
   - Onsite Servers.
   - Offsite Mirror Servers.
   - Extranets and the Cloud.

8. These items are not exhaustive and will constantly be reviewed as information processing and storage technology evolves and progresses.

Information management principles

9. The following principles underpin our management and use of information within SFC:

   - Information is an asset that has a value to SFC and should be managed accordingly.
   - Information is accessible and is shared across the organisation to increase knowledge and understanding and improve our effectiveness.
   - Information is managed properly and has an 'owner' who is responsible for its quality.
   - Data and information is defined consistently throughout SFC, and its definitions are understandable and available to all staff.
   - Data and information is secure and protected from unauthorised access, use, and disclosure, and managed in accordance with the principles set out below.

Cyber Security Essentials

10. Cyber Essentials is a Government-backed scheme of the UK National Cyber Security Centre, which helps organisations protect themselves against online threats. This involves satisfying the following five basic requirements:

    - **The use of a firewall to secure your internet connection**. This creates a safety barrier between your network and the outside world.

- **Selecting the most secure settings for your devices and software**. Often the default settings for software and devices are pre-configured to be as open as possible. It is important to re-configure these to make them secure, including the use of two factor authentication where appropriate.
- **Restrict access to data and services.** It is important to ensure that staff have appropriate access and to review user access on a regular basis.
- **Protect data with appropriate anti-virus and anti-malware.** It is essential to install appropriate anti-virus software along with anti-malware software to reduce external threats and to ensure that definitions are updated regularly.
- **Keep your software and devices up to date.** This can be achieved using patch management software which ensures all security patches are applied accordingly.

11. To achieve Cyber Essentials, certification involves a self-assessment questionnaire (SAQ) and an external independent vulnerability scan. The above recommendations are already in practice within SFC.

12. We are aiming to achieve Cyber Essentials Plus certification by the end of 2018 which involves an additional internal scan and on-site assessment.

Information security principles

13. We will ensure that we manage effectively:

    - The integrity of our information to ensure its completeness and accuracy.
    - The confidentiality of personal or sensitive information.
    - The prevention of unauthorised access to, use or disclosure of our information.
    - Business continuity by protecting our information from internal and external security incidents.
    - The physical security of our information.

Records Management lifecycle

14. We will manage our records throughout the full lifecycle: from the creation or receipt of information, through to managing its use, maintaining its integrity, controlling its storage and retrieval, to its final transfer or disposal.

15. Our records management relies on:

- Regular review.
- Controlled retention.
- Controlled sharing of information.
- Controlled destruction of information

16. Such management of our information will benefit us because it will be:

    - Easily and efficiently located, accessed and retrieved.
    - Stored securely.
    - Disposed of safely and at the right time.

Why do we need to manage our information?

17. Establishing effective information management practices will help us to work as an efficient organisation and meet our statutory obligations. Our regulatory environment is further outlined in Appendix A. Whatever form the information takes, we must ensure that it is:

    - Secure.
    - Accurate.
    - Ordered.
    - Complete.
    - Up to date.
    - Useful.
    - Accessible when needed.

18. This will in turn enable us to carry out our business by:

    - Helping us make informed decisions.
    - Tracking policy changes.
    - Supporting continuity and consistency of our operations.
    - Providing an audit trail to meet regulatory and legal requirements.
    - Ensuring we operate in an open and efficient manner as outlined in our corporate plan.

Terminology and concepts

19. Below are definitions of a record and information provided by the National Archives.[1]

[1] *Records Management Guides: 1. What is Records Management?* The National Archives (March 2006)

Record

20. Recorded information, regardless of media or format, created or received in the course of individual or organisational activity, which provides reliable evidence of policy, actions and decisions.

Information

21. Organised or manipulated data, which has theme and meaning but that is not necessarily evidence of an event or decision. Information includes published works, reference material, databases and other structured or indexed collections of information as well as records and archives.

22. We define a record as information which documents an action, a policy or a decision (i.e. it records something). Good records are created at the same time or close to the event and indicate the parties involved, organisational context, author(s) and date. Some records may have signatures to authenticate them.

23. Information is a broader concept, which covers knowledge and resources that inform the owner or user. For SFC's internal purposes records are a subset of information - such that all records are information, but not all types of information are records. For example, an email may contain important information about the details of a meeting – in other words it is information held by SFC – but is not necessarily a record because it does not need to be retained.

24. However, SFC needs to comply with wider statutory requirements, including freedom of information and data protection legislation which draw no distinction between records and information, and the Public Records (Scotland) Act 2011, which defines a record as 'anything in which information is recorded in any form' and thus we need to have systems in place to manage all our information.

Roles and responsibilities

25. In 2008, Scottish Government published the results of their review on public sector Data Handling. This report contained mandatory actions for public sector bodies which included the appointment of a Senior Information Risk Owner (SIRO).

26. Our Chief Operating Officer (COO) is designated as the Senior Information Risk Owner (SIRO) and has overall executive responsibility for our information risk and will advocate for managing information risk within the management team, ensuring we have appropriate policies

and procedures, and promoting their application throughout the organisation.

27. As SIRO, the COO also has executive responsibility for the management of our Information and Communications Technology (ICT) services and its compliance with relevant legislation.

28. Our Directors are responsible for:

- Ensuring that information security and management activities are carried out by staff and any temporary/contract personnel or consultants within their directorate in accordance with our policies, procedures and guidance.
- Encouraging good information security and management practices amongst their staff when handling our information.
- Ensuring the accuracy and integrity of information for which their staff are responsible.
- Ensuring for these functions are appropriately resourced.

29. Our Information Systems Unit (ISU) team is responsible for:

- Ensuring that staff are aware of our information security policies and procedures and their responsibilities.
- Maintaining the ICT infrastructure to support the management of our information.
- Ensuring the availability, long-term integrity and confidentiality of information stored on our ICT infrastructure.
- Maintaining suitable backup copies of all necessary information stored on our ICT infrastructure.
- Ensuring our ICT infrastructure is provided with reliable and up-to-date software and firmware.
- The safe and secure destruction of storage devices and ICT equipment at the end of their life in accordance with the Waste Electrical and Electronic Equipment Recycling standards (WEEE).
- Providing advice and guidance on information security and potential threats to management and staff.
- Monitoring the implementation of our information security policies and procedures.
- Ensuring SFC is compliant with 'Cyber Essentials'.

30. The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and requires public bodies to appoint a Data Protection Officer (DPO). SFC has designated the Information Management and Governance Officer as SFC's Data Protection Officer (DPO). The full

responsibilities of the DPO are included in SFC's Data Protection Policy. The responsibilities are to:

- Inform and advise SFC and its employees of their obligations under GDPR and UK data protection law.
- Monitor compliance with GDPR, and UK data protection law and with the policies of SFC in relation to the protection of personal data
- Provide advice where necessary on data protection impact assessments.
- Act as a point of contact with the Information Commissioners Office including when prior consultation is required before undertaking high risk processing of personal data.
- Monitor the risks associated with the processing of personal data at SFC.

31. In addition to the DPO role, the Information Management and Governance Officer is also responsible for:

- Developing and updating our wider information management and information security policies and procedures to meet our needs and obligations.
- Ensuring that staff are aware of our policies and procedures and their records management and freedom of information responsibilities.
- Giving information management advice and guidance to staff
- Monitoring the implementation of our information management policies and procedures.
- Managing the Records Management function of the Livelink Electronic Documents and Records Management (EDRM) system including the safe and timely electronic destruction of records within, the destruction of hardcopy, the management of offsite archive services, and deposits to the National Archives of Scotland.

32. Our Finance and Facilities teams are responsible for:

- Ensuring the physical security of our premises and the information infrastructure within them.
- The safe and secure disposal of confidential waste.

33. All employees are responsible for:

- Ensuring the accuracy, integrity, safe keeping and lifecycle management of any corporate information in accordance with our information security and management policies and procedures.

- Ensuring the physical security of our information for which they are responsible.
- Preserving the confidentiality of their passwords for our ICT services (except where there is an operational need; e.g. a manager may tell their assistant their PIN to access their voicemail).
- Immediately reporting any security incident or data breach to our IMGO as well as the IS or Facilities team as appropriate.

Review of the Framework

34. The Assistant Director (Strategy) has overall day-to-day responsibility for Records Management and will be responsible for ensuring the review of this Information Management Framework annually.

Related policies and procedures

35. This framework should be read in conjunction with the following SFC policies and procedures, which cover differing aspects of information management in further detail.

    - Data Protection policy.
    - External Data Processing policy.
    - Data Breach procedures.
    - Information Security policy
    - Remote Working policy.
    - Acceptable use policy.
    - Monitoring policy.
    - Business continuity plan.
    - Staff code of conduct.
    - Records Management Staff Manual.
    - Retention and Disposal policy.
    - LINKS user manual.
    - Freedom of Information policy.

Document Control

Title	Information Management Framework
Prepared By	Information Management and Governance Officer
Approved Internally By	Chief Operating Officer
Date of Approval	20 March 2019
Version Number	1.5
Review Frequency	Annually
Next Review Date	March 2020

Version control

Version	Date	Control Reason	Author
1.1	21-07-14	Minor re-drafting	Richard Hancock
1.2	30-10-14	Minor re-drafting	Alison Kendall
1.3	20-05-15	General review: minor changes	Alison Kendall
1.4	15-10-15	Re-drafting to list additional relevant policies and reference to current information processing practices and formats. Additional detail to explain responsibilities for record destruction. Minor changes reflecting new SFC structure October 2015.	Simon Macauley
1.5	16-02-18	Re-drafting to take account of GDPR implementation and Cyber Security Essentials and update to role of SIRO as well as minor updates throughout.	Callum Morrison
1.6	10-09-18	Minor re-drafting after implementation of Data Protection Act 2018. Inclusion of a policy diagram.	Callum Morrison

Appendix A: our regulatory environment

36. We work in a regulatory environment influenced by many factors including those listed below. Our information management policies and procedures need to incorporate the resulting regulatory and statutory obligations.

37. Statute, case law and regulations including, but are not limited to:

- Data Protection Act 2018
- EU General Data Protection Regulation 2016/679
- Privacy and Electronic Communications Regulations 2003
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- Reuse of Public Sector Information Regulations 2005
- Electronic Communications Act 2000
- Regulation of Investigatory Powers (Scotland) Act 2000
- Lawful Business Practice Regulations 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Public Records (Scotland) Act 1937
- Public Records (Scotland) Act 2011

38. Codes of best practice; for example:

- Codes of practice under Sections 60 and 61 of the Freedom of Information (Scotland) Act 2002.
- Department of Constitutional Affairs Guidance on Public Sector Data Sharing (November 2003).
- Information and documentation – Records management, BS ISO 15489 2001.
- Information technology. Security techniques. Information security management systems. Requirements. BS ISO/IEC 27001:2005 (BS 7799-2:2005).
- European Data Protection Board[1] and ICO codes of best practice.
- The SFC staff code of conduct

[1] The European Data Protection Board replaced the Article 29 Working Party on Data Protection with the implementation of the GDPR. The European Data Protection Board replaced the Article 29 Working Party on Data Protection with the implementation of the GDPR.

Appendix B: related policies and procedures