Information Management Framework
### Document Control

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Information Management Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepared By</strong></td>
<td>Information Management and Security Officer</td>
</tr>
<tr>
<td><strong>Approved Internally By</strong></td>
<td>Assistant Director for Learning, Governance and Sustainability</td>
</tr>
<tr>
<td><strong>Date of Approval</strong></td>
<td>01-06-2014</td>
</tr>
<tr>
<td><strong>Review Frequency</strong></td>
<td>Biennially</td>
</tr>
</tbody>
</table>

### Version control

<table>
<thead>
<tr>
<th><strong>Version</strong></th>
<th><strong>Date</strong></th>
<th><strong>Control Reason</strong></th>
<th><strong>Author</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>21-07-14</td>
<td>Minor re-drafting</td>
<td>Richard Hancock</td>
</tr>
<tr>
<td>1.2</td>
<td>30-10-14</td>
<td>Minor re-drafting</td>
<td>Alison Kendall</td>
</tr>
<tr>
<td>1.3</td>
<td>20-05-15</td>
<td>General review: minor changes</td>
<td>Alison Kendall</td>
</tr>
<tr>
<td>1.4</td>
<td>15-10-15</td>
<td>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.</td>
<td>Simon Macauley</td>
</tr>
<tr>
<td>1.5</td>
<td>27-07-16</td>
<td>No Changes</td>
<td>Simon Macauley</td>
</tr>
</tbody>
</table>
Introduction

1 This framework, together with its underpinning policies and procedures, outlines how we will manage our corporate information to ensure the best use and storage of this resource and to comply with our statutory obligations. The framework has two main threads:

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

What does this framework cover?

2 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.

3 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

4 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

5 These bulleted items are not exhaustive and will constantly be reviewed as information processing and storage technology evolves and progresses.
Information management principles

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

- Information is an asset that has 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.

Information security principles

7 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

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

9 Our records management relies on
• Regular review
• Controlled retention
• Controlled destruction of information

10 Such management of our information will benefit us as 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?

11 Establishing effective information management practices will help us work as an efficient organisation and meet our statutory obligations. Our regulatory environment is further outlined in Appendix 1. Whatever form the information takes, we must ensure it is:

• Secure
• Accurate
• Ordered
• Complete
• Up to date
• Useful
• Accessible when needed

12 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

Below are definitions of a record and information as given by the National Records Office.¹

**Record**

*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**

*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.*

A record is information that 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.

Information is a broader, amorphous concept, which covers knowledge and resources that inform the owner or user. Records are a subset of information such that all records are information but not all types of information are records.

However, we need to comply with Freedom of Information legislation which draws no distinction between records and information and thus we need to have systems in place to manage all our information.

**Who does this framework apply to?**

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.

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.

¹ Records Management Guides: 1. What is Records Management? The National Archives (March 2006)
Staff will have access to information management training and we will provide supporting procedures and guidelines for them. We will review our policies regularly to ensure they continue to be relevant.

Roles and responsibilities

Our Chief Executive has overall executive responsibility for our information management, ensuring we have appropriate policies and procedures, and promoting their application throughout the organisation. Our Director of Corporate Services has responsibility for the management of our Information and Communications Technology (ICT) services and its compliance with legislation.

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

Our Information Systems (IS) 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

23 The Information Management and Security Officer is responsible for:

• Developing and updating our 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 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 EDMS system including the safe and timely electronic destruction of records within the EDMS, the destruction of hardcopy, the management of offsite archive services, and deposits to the National Archives of Scotland.

24 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

25 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 to our IS or Facilities team. Data breaches should be reported to the IMSO.

**Monitoring of our information management policies**

26 We will undertake periodic monitoring to ensure compliance with our information management policies. The monitoring will take the form of an annual timetable of checks and interviews with staff and, where appropriate, external parties, and will focus on areas of high-risk to the organisation. The monitoring will be undertaken by the Information Management and Security Officer.

27 Appendix 2 sets out our planned timetable of monitoring for 2016-17.

**Review of the Framework**

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

**Related policies and procedures**

29 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
Appendix 1

Our regulatory environment

1 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.

(i) Statute, case law and regulations including, but are not limited to:

- 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
- Data Protection Act 1998
- The 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

(ii) 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

(iii) The SFC staff code of conduct.
<table>
<thead>
<tr>
<th>Item Number</th>
<th>Information Policy Monitoring 2015-16 and 2016 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Policy</td>
</tr>
</tbody>
</table>
| 1           | External Data Processing Policy | Staff do not contact the IMSO or carry out a PIA when tendering or commissioning external agents to process SFC personal data. | • Policy reinforced during HR Induction and DP training  
• SFC terms and conditions and SFC data Protection policy both refer to the EDP and the need for PIAs  
• Annual review | Meet regularly with key data asset owners to discuss any plans for data sharing:  
Planned meetings March 2016:  
• Gordon McBride AD for Funding;  
• Ian McCracken Head of HR |
| 2 | Information Security Policy | • Transfers of personal data  
• Safe data and hardware disposal  
• Physical security  
• Firewalls and anti-virus software | • Policy reinforced during HR Induction and DP training  
• Emails notices on salient current alerts and incidents  
• Annual review | Liaise closely with Head of ICT holding quarterly meetings to discuss any issues regarding overall ICT security.  
Meet and liaise regularly with Facilities Officer to discuss state of safe destruction and physical access.  
Planned meetings March 2016:  
• Head of ICT  
• Facilities Officer |
| 3 | Remote Working Policy | • Integrity of VPN  
• Encryption of SFC loaned devices | • Policy reinforced during HR Induction and DP training  
• Emails notices on salient current alerts and incidents  
• Annual review | Liaise closely with Head of ICT holding quarterly meetings to discuss any issues regarding remote working.  
Meeting with Head of ICT scheduled for March 2016. |
| --- | --- | --- | --- | --- |
| 4 | Data Protection Policy | • Privacy Impact Assessments (PIAs)  
• Staff management of their own data  
• Staff and management responsibilities | • Policy reinforced during HR Induction and DP training  
• Emails notices on salient current alerts and incidents  
• Annual review | Liaise closely with Head of HR. Meet six-monthly to discuss and recognise any need for PIAs re staff data processing.  
Contacting Heads of directorate six-monthly to remind of the need to carry out PIA if required.  
|   | Retention and Disposal policy | Accurate synchronising of file plan and appropriate retention periods.  
|   |  | EDMS disposition runs |
|   | Current rolling review of branch retention periods and file plan mapping. 2015-end 2016. |
|   | Responsibility of the IMSO who reports to AD (Strategy) at Quarterly team meetings. |
|   | Monitoring Policy | Clarity of procedures for staff and responsibilities for line managers and IT staff. |
|   |  | Policy reinforced during HR Induction and DP training  
|   |  | Links to the SFC data Protection and Acceptable Use policies  
|   |  | Annual review |
|   |  | Liaise closely with Head of HR and ICT to ensure any changes to corporate policy are reflected by amendments.  
|   |  | Annual meeting with Heads of ICT and HR. scheduled for March 2016. |
|   | Acceptable Use Policy | The SFC is potentially vulnerable if systems and working practices are degraded by not making clear to staff the rules for users on ICT systems. |
|   |  | Policy reinforced during HR Induction and DP training  
|   |  | Links to the SFC data Protection  
|   |  | Annual review |
|   |  | IMSO annual meeting with Head of HR. Scheduled for March 2016. |