Scottish Funding Council

Promoting further and higher education

Records Management Plan

October 2014

Document control

Title	The Scottish Funding Council Records Management Plan
Prepared by	Information Management and Security Officer
Approved internally by	Martin Fairbairn, Senior Information Risk Owner
Date of approval	July 2014
Version number	1.1
Review frequency	Annually for the first two years and thereafter biennially
Next review date	July 2015

Version control

Version	**Date**	**Status**	**Prepared by**	**Reason for Amendment**
1.0	July 2014	Final	Simon Macauley	
1.1	October 2014	Final	Alison Kendall	Amended to address points raised in the Keeper's interim report

The Keeper of the Records of Scotland will be alerted to any changes that are made to this Records Management Plan in accordance with section 5(6) of the Public Records (Scotland) Act 2011.

Contents

The SFC Records Management Plan

Introduction

The Scottish Further and Higher Education Funding Council (SFC) is the national, strategic body with responsibility for funding teaching and learning provision, research and other activities in Scotland's 25 colleges and 19 universities and other higher education institutions. We are more commonly known as 'the Scottish Funding Council' or 'SFC'.

SFC is a Non-Departmental Public Body (NDPB) of the Scottish Government and was established on 3 October 2005. Our statutory duty is to secure coherent, high quality further and higher learning provision by colleges and universities in Scotland, and the undertaking of research. We do this by investing in the development of a coherent college and university system which, through enhanced learning, research and knowledge exchange, leads to improved economic, educational, social, civic and cultural outcomes for the people of Scotland.

Under the Public Records (Scotland) Act 2011, Scottish public authorities must produce and submit a records management plan (RMP) setting out proper arrangements for the management of an authority's public records to the Keeper of the Records of Scotland for his agreement under section 1 of the Act. As a major public body in Scotland – with an annual budget of about £1.5 Billion – effective records management is essential to the success of our organisation and its effectiveness.

SFC has a mature records management environment. Recognising the benefits of good records management, we implemented a combined intranet and Electronic Document and Records Management System (EDRMS) in 2007 and a deliberate strategy of managing records electronically. The EDRMS, which was provided by Opentext and is called LINKS, has enabled us to centralise all our record management functions, including the managed retention and disposal of electronic and physical objects. LINKS ensures that our records are held and managed in a structured format and are accessible across the organisation, except where there is a business need to restrict access.

As part of the work to introduce an EDRMS, we developed a functional, corporate file plan, which we have used as a basis for developing the Records Management Plan (RMP) set out in this document. The scope of this Plan covers all records, including both physical and electronic.

To compliment this RMP, we have updated our key information management policies and are implementing a rolling review of our record management processes. We will continue to enhance and develop our record management systems in collaboration with National Records Scotland.

Our Records Management plan

Our RMP sets out the framework for ensuring that SFC's records are managed and controlled effectively, commensurate with the legal, operational and information needs of the organisation. The RMP covers all 14 elements in the Keeper's Model RMP and supporting guidance material:

1. Senior management responsibility
2. Records Manager responsibility
3. Records management policy statement
4. Business classification
5. Retention schedules
6. Destruction arrangements
7. Archiving and transfer arrangements
8. Information security
9. Data protection
10. Business continuity and vital records
11. Audit trail
12. Competency framework for records management staff
13. Assessment and review
14. Shared information

The 14 elements of the plan are set out in the rest of this document.

Element 1: Senior Management Responsibility

Introduction	A mandatory element of the Public Records (Scotland) Act 2011, senior management responsibility is the single, most important piece of evidence to be submitted as part of the Records Management Plan. This element must identify the person at senior level who has overall strategic responsibility for records management within the organisation.
Statement of Compliance	The Senior Responsible Officer for Records Management within The Scottish Funding Council who has delegated strategic responsibility for Records Management is Martin Fairbairn, the Senior Director for Institutions and Corporate Services, who is also the organisation's Senior Information Risk Owner (SIRO). Day-to-day management responsibility is the responsibility of Richard Hancock, Assistant Director for Learning, Governance and Sustainability.
Evidence of Compliance	Evidence to be submitted in support of Element 1: • Item 001: SFC Information Management Framework
Future Developments	There are no planned future developments in respect of Element 1. However, if the Senior Responsible Officer for Records Management were to change, we would revise our policies and procedures.
Assessment and Review	This element will be reviewed if there any changes in personnel.
Responsible Officer(s)	Laurence Howells, Chief Executive

Element 2: Records Manager Responsibility

Introduction	A mandatory element of the Public Records (Scotland) Act 2011, the plan must identify the individual with operational responsibility for Records Management within the organisation.
Statement of Compliance	The officer with operational responsibility for Records Management within the Scottish Funding Council: • Information Management and Security Officer: Simon Macauley
Evidence of Compliance	Evidence to be submitted in support of Element 2: • Item 001: SFC Information Management Framework • Item 002: IMSO Competency Framework
Future Developments	No developments are planned at this time.
Assessment and Review	This element will be reviewed if there are any changes in personnel.
Responsible Officer(s)	Richard Hancock, Assistant Director for Learning, Governance and Sustainability

Element 3: Records Management Policy Statement

Introduction	A Records Management Policy Statement (RMPS) must demonstrate the importance of managing records within the organisation and serve as a mandate for the activities of the Information Management and Security Officer. The RMPS provides an overarching statement of the organisation's priorities and intentions in relation to recordkeeping, and a supporting framework and mandate for the development and implementation of a RM culture within the organisation.
Statement of Compliance	An overarching Information Management Framework outlining the records management and information assurance processes in place for the SFC was approved by the organisation's Chief Executive's Group (CEG) in 2008. The Information Management Framework describes how SFC manages its records in line with the business functions of the organisation, best practice, and regulatory and legal requirements.
Evidence of Compliance	Evidence to be submitted in support of Element 3: • Item 001: SFC Information Management Framework
Future Developments	There are no planned future developments in respect of Element 3. However, the policy is reviewed at least annually in order to ensure that it continues to reflect best practice and current practice within SFC.
Assessment and Review	This element is reviewed annually by the Information Management and Security Officer.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Element 4: Business Classification

Introduction	The Keeper expects an organisation to carry out a comprehensive assessment of its core business functions and activities, and represent these within a Business Classification Scheme (BCS). Element 4 of the RMP should confirm that the organisation has developed, or is in the process of developing, a BCS.
Statement of Compliance	SFC carried out a comprehensive assessment of its core business functions and activities in 2007 to prepare the way for the introduction of its EDRMS. The current Corporate File Plan is based on Functionality, Activity, and Task (FAT), and provides a structure for managing records through their lifecycle from creation to disposal. The Information Management and Security officer is responsible for maintaining the FAT File Plan. No functions of SFC are carried out by third-parties.
Evidence of Compliance	Evidence to be submitted in support of Element 4: • Item 003: SFC Corporate File Plan
Future Developments	No developments are planned at this time.
Assessment and Review	The SFC Corporate File Plan is reviewed annually.
Responsible Officer(s)	Simon Macauley, Information Management and Security officer.

Element 5: Retention Schedules

Introduction	Retention schedules must demonstrate the existence of, and adherence to, corporate records retention procedures. These procedures should show that the organisation routinely disposes of information, whether this is destruction or transfer to an archive for permanent preservation. A retention and disposal schedule which sets out recommended retention periods for records created and held by an organisation is essential for ensuring that the organisation's records: • Are not retained for longer than necessary (in line with legal, statutory and regulatory obligations) • Storage costs are minimised (through the timely destruction of business information) • Records that are deemed worthy of permanent preservation are identified and transferred to an archive at the earliest opportunity
Statement of Compliance	The SFC has developed a Retention and Disposal Schedule, which has been mapped to the functional structure of the Corporate File Plan. The Schedule ensures that retention rules are applied consistently across SFC's functions and extends to all records in the organisation.
Evidence of Compliance	Evidence to be submitted in support of Element 5: • Item 004: Retention and Disposal Schedule
Future Developments	The Retention and Disposal Schedule is currently being reviewed and we expect any changes to be completed by March 2015. We have some legacy hardcopy records which are kept either onsite or at Iron Mountain. We are about to establish a temporary post to review all onsite and offsite storage of records and documents with a view to ensuring that all such records are recorded in the LINKS EDRMS with appropriate retention and disposal schedules, or destroyed where they no longer need to be retained for business purposes.
Assessment and Review	The Information Management and Security Officer is responsible for monitoring and reviewing the Schedule when

	any changes are requested or required, ensuring that it continues to reflect record-keeping best practice as well as meeting legal and statutory obligations.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer Richard Hancock, Assistant Director for Learning, Governance and Sustainability

Element 6: Destruction Arrangements

Introduction	A mandatory element of the Public Records (Scotland) Act 2011, Destruction Arrangements should evidence the arrangements that are in place for the secure destruction of confidential information. Clear destruction arrangements setting out the correct procedures to follow when destroying business information are necessary in order to: • Minimise the risk of an information security incident • Ensure that the organisation meets its obligations in relation to the effective management of its records, throughout their lifecycle
Statement of Compliance	**Physical records held onsite** The Retention and Disposal Policy sets out the procedures for disposing of records within SFC. We have a detailed contract with 'Shred-It', which describes the methods used in the on-site destruction of physical records, including hardware. **Records held offsite** For paper records held offsite at Iron Mountain, destruction can be arranged by providing a destruction list and a signed preliminary form (provided by Iron Mountain). Destruction is carried out by supervised secure shredding and destruction certificates are provided. **Backups** Services and data are backed up nightly using a dedicated rack at Saughton Data Centre that has a 1GB LAN extension connected to it from the SFC site. This allows us to run production services from Saughton and lets us replicate and backup our services and data to the Saughton rack overnight. The backups are run on a daily, weekly, monthly cycle and are automatically overwritten as part of the cycle.
Evidence of Compliance	Evidence to be submitted in support of Element 6: • Item 004: Retention and Disposal Policy • Item 005: Shred-It Customer service agreement • Item 006: Shred-It Customer service agreement hardware (one-off) • Item 018: ICT Equipment Disposal policy

	• Item 019: Annex G to Business Continuity Plan – SFC ICT continuity strategy
Future Developments	No developments are planned at this time.
Assessment and Review	We will review the destruction arrangements when our existing contract for secure off-site storage of documents is re-tendered later in 2014.
Responsible Officer(s)	• Simon Macauley, Information Management and Security Officer (Item 004) • Fiona O'Neill, Assistant Director for Finance and Corporate Resources (Item 005 and 006) • Laurence McDonald, Head of Information Systems (Item 018)

Element 7: Archiving and Transfer Arrangements

Introduction	A mandatory element of the Public Records (Scotland) Act 2011, Archiving and Transfer Arrangements should detail the processes in place within an organisation to ensure that records of long-term historical value are identified and deposited with an appropriate archive repository. Arrangements for the transfer of material of enduring value to an archive should be clearly defined and made available to all staff in order to ensure that: • The records are transferred at their earliest opportunity • The corporate memory of the organisation is fully and accurately preserved
Statement of Compliance	Council Board and Council committee papers and official communications – which record formal decisions taken by, and formal communications from, SFC – are sent as hardcopy to the National Records of Scotland (NRS) for permanent preservation.
Evidence of Compliance	Evidence to be submitted in support of Element 7: • Item 007: Deposit Agreement with NRS
Future Developments	We are proposing to transfer records electronically to NRS for archiving in future and are currently testing our EDRMS to develop an effective method of transfer.
Assessment and Review	The SFC's Archiving and Transfer Arrangements are reviewed annually by the Information Management and Security Officer in conjunction with the Keeper's client managers.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Element 8: Information Security

Introduction	Information security policies and procedures are essential in order to protect an organisation's information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. A mandatory element of the Public Records (Scotland) Act 2011, Information Security should set out provisions for the proper level of security of its records and ensure that there is evidence of robust information security procedures, which are well understood by all members of staff.
Statement of Compliance	SFC has a suite of information security policies, which are approved by the Chief Executive of SFC and are reviewed on an annual basis. Any changes to the policies are communicated to staff. There is also regular training for staff on information security and data protection, which emphasises the importance of good records management.
Evidence of Compliance	Evidence to be submitted in support of Element 8: • Item 009: SFC Information Security Policy • Item 010: Data Protection and Information Security PowerPoint presentation • Item 011: SFC Remote Working Policy • Item 012: SFC External Data Processing policy
Future Developments	No developments are planned at this time.
Assessment and Review	The policies are updated as necessary by the Information Management and Security Officer and formally at least annually. All staff will be informed if there are any changes to policies and procedures.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Element 9: Data Protection

Introduction	The Keeper expects an organisation to provide evidence of compliance with data protection responsibilities for the management of all personal data.
Statement of Compliance	SFC has a legal obligation to comply with the requirements of the Data Protection Act 1998 in relation to the management, processing and protection of personal data. SFC's Data Protection Policy is a statement of responsibility and demonstrates the organisation's commitment to compliance with the Act and the safeguarding and fair processing of all personal data held by SFC. SFC has submitted a notification to the Information Commissioner for inclusion in the Data Protection Public Register annually since 2005 and provides in-house training for staff on data protection awareness. Compliance with the Data Protection Act is the responsibility of the Information Management and Security Officer.
Evidence of Compliance	Evidence to be submitted in support of Element 9: • Item 009: SFC Information Security Policy • Item 013: SFC Data Protection Policy • Item 010: DP, Information Security PowerPoint presentation • Item 011: SFC Remote Working Policy • Item 012: SFC External Data Processing policy • Item: 014: SFC Acceptable Use Policy
Future Developments	No developments are planned at this time.
Assessment and Review	The policies are reviewed formally each year ensuring that they remain accurate and up-to-date. The register entry is regularly monitored and updated as necessary.
Responsible Officer(s)	• Simon Macauley, Information Management and Security Officer • Martin Fairbairn, Senior Director for Institutions and Corporate Services

Element 10: Business Continuity and Vital Records

Introduction	It is recommended that a Business Continuity and Vital Records Plan is in place in order to ensure that key records and systems are protected and made available as soon as possible in the event of, and following, an emergency. The plan should identify the measures in place to prepare for, respond to, and recover from such an emergency.
Statement of Compliance	SFC has a Business Continuity Plan (BCP) which is agreed by SFC's Audit and Compliance Committee. (The Business Continuity Plan is part 6 of the Financial Procedures Manual, but acts as a standalone document.) As all of SFC's electronic records are backed up regularly, specific identification of vital records is not felt to be necessary.
Evidence of Compliance	Evidence to be submitted in support of Element 10: • Item 008: Minutes of the Audit and Compliance Committee Meeting in which the Business Continuity Plan was agreed • Item 015: Business Continuity Plan (BCP) • Item 020: Annex F to Business Continuity Plan – Testing Schedule
Future Developments	No developments are planned at this time.
Assessment and Review	Testing of the BCP is undertaken annually. A management review of the BCP is carried out annually or when there is any form of major change within the organisation or significant development which may have an impact on business continuity.
Responsible Officer(s)	Laurence Howells, Chief Executive.

Element 11: Audit Trail

Introduction	An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities. The Keeper will expect an authority's records management system to provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record.
Statement of Compliance	SFC already includes a full auditing function of electronic records within its EDRMS. We use structured corporate drives for managing certain functions – such as the processing and modelling of statistical data mainly in excel spreadsheets. However, any records are saved into LINKS, our EDRMS. Records held at Iron Mountain are stored in boxes. We hold a spreadsheet detailing the box number, group and member of staff responsible with dates due for destruction and/or review. There are also paper inventories which detail what is stored in each box so that individual records can be located and, if necessary, recalled from storage. When a box is recalled, a note is made in the inventory and the spreadsheet is amended to document this, including details of who has requested the box. For hard copy records stored onsite, currently each group within SFC keeps their own inventory of what is held. A 'physical objects' EDRMS module has been developed to enable staff to log records currently kept as hard copies. This is currently being tested and should be live by the end of 2014.
Evidence of Compliance	Primary evidence to be submitted in support of Element 11 includes: • Item 001: SFC Information Management Framework • Item 004: Retention and Disposal policy • Item 016 : Links EDRMS Manual
Future	We have some legacy hardcopy records which are kept either

Developments	onsite or at Iron Mountain. We are about to establish a temporary post to review all on and offsite storage of records and documents with a view to ensuring that all such records are recorded in the LINKS EDRMS with appropriate retention and disposal schedules and auditing of any changes.
Assessment and Review	Reviewed as required by Audit Scotland and internal audit reports.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Element 12: Competency Framework for Records Management Staff

Introduction	Core competencies and key knowledge and skills required by staff with responsibilities for Records Management should be defined clearly and made available within organisations, to ensure that staff understand their roles and responsibilities, can offer expert advice and guidance, and can remain proactive in their management of recordkeeping issues and procedures. With core competencies defined, the organisation can identify training needs, assess and monitor performance, and use them as a basis from which to build future job descriptions.
Statement of Compliance	The SFC Information Management and Security Officer (IMSO) Competency Framework defines the role and responsibilities of the IMSO.
Evidence of Compliance	Evidence to be submitted in support of Element 12: • Item 002: IMSO Competency Framework
Future Developments	RM training is included as core requirement in the Job Profile and Forward Job Plan of the Information Management and Security Officer.
Assessment and Review	Training programs are regularly updated to comply with legislation and appropriate codes of practice. The Assistant Director for Learning, Governance and Sustainability reviews biannually the training requirements of the Information Management and Security Officer.
Responsible Officer(s)	• Simon Macauley, Information Management and Security Officer • Richard Hancock, Assistant Director for Learning, Governance and Sustainability

Element 13: Review and Assessment

Introduction	Records Management practices within an organisation must remain fit for purpose and procedures closely monitored, assessed and reviewed to ensure compliance and commitment to best practice in recordkeeping. The Keeper expects the Records Management Plan to identify mechanisms for regularly reviewing the contents of the Plan and for ensuring that processes are operating effectively.
Statement of Compliance	SFC's information governance policies and procedures, which support the requirements of the Public Records (Scotland) Act 2011, are reviewed by the Information Management and Security Officer (IMSO) annually or as required to ensure compliance with all business as well as legal obligations. The Records Management Plan will be reviewed by the IMSO annually for the first two years and thereafter biennially.
Evidence of Compliance	Evidence to be submitted in support of Element 13: • Item 001: Information Management Framework • Item 020: Annex F to Business Continuity Plan – Testing Schedule • Item 021: Draft Guidelines for reviewing the SFC Records Management Plan
Future Developments	A review structure is being developed to check the organisation's Information and Records Management practices against the 14 elements of the RMP to ensure we are meeting our regulatory and statutory obligations and are implementing best practice. Reviews will be carried out by the IMSO and approved by the Chief Executive.
Assessment and Review	The policies and procedures supporting the requirements of the Public Records (Scotland) Act 2011 are reviewed annually or as required.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Element 14: Shared Information

Introduction	Procedures for the efficient sharing of information both within an organisation and with external partners are essential for ensuring information security and recordkeeping compliance. Protocols should include guidance as to what information can be shared, who should retain the data, what levels of security are to be applied, who should have access, and the nature of the disposal arrangements.
Statement of Compliance	SFC operates in accordance with the UK Information Commissioner's Data Sharing Code of Practice. A standard Data Access Agreement template is also in existence within the organisation, which can be modified to reflect the specific requirements and circumstances of sharing information. SFC also has a policy on the external processing of data which directs employees on the safe and secure process when tendering or commissioning outside agencies to process data on our behalf. SFC has only one platform for sharing information called 'Secure-Send'. This is a browser platform on an SFC server onto which colleges upload statistical information. Data sharing agreements determine the retention periods and disposition procedures for statistical data that is no longer required by SFC.
Evidence of Compliance	Evidence to be submitted in support of Element 14: • Item 012: External Data Processing Policy • Item 017: Data Access/Sharing Agreement Template
Future Developments	No developments are planned at this time.
Assessment and Review	The SFC data sharing agreement is customised for appropriate use for each data sharing project undertaken at the time of commission.
Responsible Officer(s)	Simon Macauley, Information Management and Security Officer.

Annex A: Evidence to be submitted

Please find below a list of evidence to be submitted in support of each of the elements of the Records Management Plan below. This evidence will be submitted separate to this Records Management Plan, in paper format.

EVIDENCE ITEM REF NO.	DETAILS	DATE	IN SUPPORT OF ELEMENT(S)
001	SFC Information Management Framework	October 2014	1, 2, 3, 11, 13
002	IMSO Competency Framework	June 2012	2, 12
003	SFC Fileplan: Functionality, Activity, and Task (FAT).	2007	4
004	Retention and Disposal policy	2007	5, 6, 11
005	Shred-It Customer Service Agreement	Oct 2012	6
006	Shred-It Customer Service Agreement (Hard drives)	February 2014	6
007	Deposit Agreement with NAS	2014	7
008	Minutes of the Audit and Compliance Committee Meeting in which the Business Continuity Plan was agreed	December 2012	10
009	Information Security Policy	July 2014	8, 9
010	DP and Information Security PowerPoint presentation	2014	8, 9
011	SFC Remote working policy	July 2014	8, 9
012	SFC External Data Processing policy	July 2014	8, 9, 14
013	SFC Data Protection Policy	July 2014	9
014	SFC Acceptable Usage policy	2010	9
015	SFC Business Continuity Plan	March 2013	10
016	LINKS User Manual	2012	11
017	Data Access/Sharing Agreement Template	2010	14
018	SFC ICT Equipment Disposal policy	2010	6
019	Annex G to Business Continuity Plan – SFC ICT continuity strategy	March 2013	6
020	Annex F to Business Continuity Plan – Testing Schedule	March 2013	10, 13
021	Draft Guidance for reviewing the SFC Records Management Plan	October 2014	13