National Records of Scotland

Records Management Plan of Registrar General for Scotland and Keeper of the Records of Scotland (National Records of Scotland)

November 2017

Document Control

Title	NRS Records Management Plan
Prepared By	Head of Records Management
Approved Internally By	Head of Data Resources
Date of Approval	16 November 2017
Version Number	3.4
Review Frequency	Annually
Next Review Date	June 2018

Status Control

Version	Date	Status	Prepared by	Reason for Amendment
1.0	11 April 2013	Final	John Simmons	
2.0	10 May 2013	Final	John Simmons	To update target dates for delivery of records management programme.
3.0	22 July 2016	Final	John Simmons	To reflect staff changes, developments in strategy and overall progress.
3.1	04 January 2017	Final	John Simmons	Update to Element 8.
3.2	20 February 2017	Final	John Simmons	Change to senior responsible officer for records management and business continuity leader.
3.3	02 June 2017	Final	John Simmons	Update to Element 14 and minor updates to some other elements.
3.4	16 November 2017	Final	John Simmons	To reflect staff changes

CONTENTS

Introduction		4
Element 1:	Senior management responsibility	5
Element 2:	Records manager responsibility	6
Element 3:	Records management policy statement	7
Element 4:	Business classification	8
Element 5:	Retention schedules	9
Element 6:	Destruction arrangements	11
Element 7:	Archiving and transfer arrangements	12
Element 8:	Information security	14
Element 9:	Data protection	16
Element 10:	Business continuity and vital records	18
Element 11:	Audit trail	20
Element 12:	Competency framework for records management staff	22
Element 13:	Review and assessment	24
Element 14:	Shared information	25
ANNEX A	Evidence submitted	27

INTRODUCTION

This is the Records Management Plan (RMP) of the Registrar General for Scotland and the Keeper of the Records of Scotland.

The Public Records (Scotland) Act 2011 obliges named authorities to prepare and implement a RMP setting out proper arrangements for the management of their corporate records. The offices of Registrar General and Keeper of the Records are separately named as authorities in the schedule of the Act. These offices are currently held by the Chief Executive of National Records of Scotland (NRS). A combined RMP was submitted in April 2013 and agreed by the Keeper in June 2013. The RMP agreed by the Keeper has been previously published on the NRS website.

Although the Chief Executive will not be invited to resubmit the RMP for agreement until at least 2018, changes will continue to be made to its content as new corporate policies and procedures for the management of records are developed and existing ones reviewed and revised. The Keeper will be regularly alerted to any significant changes in accordance with section 5(6) of the Act.

The Records Management Plan is based on the Keeper's published Model Records Plan and has 14 Elements.

ELEMENT 1: SENIOR MANAGEMENT RESPONSIBILITY

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 1: 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 National Records of Scotland is the Head of Data Resources: Gerry Donnelly.

Evidence of Compliance

Primary evidence:

- Item 001: Statement of Responsibility for Records Management (191KB PDF)
- Item 002: Records Management Policy (50KB PDF)

Future Developments

There are no planned future developments.

Assessment and Review

This element will be reviewed as soon as there any changes in personnel.

Responsible Officer

Chief Executive of National Records of Scotland: Tim Ellis.

ELEMENT 2: RECORDS MANAGER RESPONSIBILITY

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 2: Records manager responsibility must identify the individual within the organisation, answerable to senior management, to have operational responsibility for records management within the organisation.

Statement of Compliance

The officer with operational responsibility for records management within National Records of Scotland is the Head of Records Management: John Simmons. He is responsible for the provision of records management services at all NRS sites and for managing the contract for records which are stored off site with Iron Mountain.

Evidence of Compliance

- Item 001: Statement of Responsibility for Records Management (191KB PDF)
- Item 002: Records Management Policy (158KB PDF)
- Item 003: Records Manager Job Summary (35KB PDF)

Future Developments

There are no planned future developments.

Assessment and Review

This element will be reviewed as soon as there any changes in personnel.

Responsible Officers

Head of Data Resources: Gerry Donnelly.

ELEMENT 3: RECORDS MANAGEMENT POLICY STATEMENT

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 3: Records management policy statement must demonstrate the importance of managing records within the organisation and serve as a mandate for the activities of the records manager. It is necessary in order to provide an overarching statement of the organisation's priorities and intentions in relation to recordkeeping, and deliver a supporting framework and mandate for the development and implementation of a records management culture.

Statement of Compliance

NRS recognises that the effective management of its records, regardless of format, is essential in order to support our functions, to comply with legal, statutory and regulatory obligations, and to demonstrate transparency and accountability to all of our stakeholders. Our commitment to effective records management is set out in our corporate Records Management Policy. NRS follows and complies with the best practice and guidance on the keeping, management and destruction of records set out in the Section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002.

Evidence of Compliance

- Item 002: Records Management Policy (158KB PDF)

Future Developments

There are no planned future developments.

Assessment and Review

The policy is subject to ongoing monitoring and annual review to ensure that it continues to reflect the organisational position in relation to recordkeeping.

Responsible Officer

Head of Records Management: John Simmons.

ELEMENT 4: BUSINESS CLASSIFICATION

Introduction

A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership. The Keeper expects an authority to carry out a comprehensive assessment of its core business functions and activities, and represent these within a business classification scheme.

Statement of Compliance

Following an information audit exercise in 2012-13, NRS developed a business classification scheme which identifies and describes the organisation's core functions, component activities and associated transactions. Since then NRS has decided to primarily manage its corporate information within the Scottish Government's electronic document and records management (EDRM) system, Objective eRDM. This system is configured to the Scottish Government's business classification scheme, which has been adapted from the Integrated Sector Vocabulary Scheme (IPSV). The suitability of the Scottish Government's business classification scheme for NRS was assessed and validated during the implementation of eRDM.

Evidence of Compliance

- Item 004: NRS Business Classification Scheme
- Item 005: Scottish Government Business Classification Scheme
- Item 006: Scottish Government Fileplan Levels 1 to 3
- Item 007: Extract of NRS file in eRDM

Future Developments

The Scottish Government are pursuing a project to upgrade the current eRDM system and as part of this project will consider rationalising the present business classification scheme. As a user of eRDM NRS will have the opportunity to contribute to this. If changes are made to the business classification scheme the RMP will be updated to reflect this.

Assessment and Review

The management of NRS records within this business classification scheme will be subject to ongoing monitoring and annual review to ensure that all of the functions, activities and transactions carried out by NRS continue to be represented within it.

Responsible Officer

Head of Records Management: John Simmons.

ELEMENT 5: RETENTION SCHEDULES

Introduction

A retention schedule is a list of records for which pre-determined disposal dates have been established. An authority must demonstrate the existence of and adherence to corporate records retention procedures. These procedures must 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 longer than necessary (in line with legal, statutory and regulatory obligations), storage costs are minimised (through the timely destruction of business information), and records deemed worthy of permanent preservation are identified and transferred to an archive at the earliest opportunity.

Statement of Compliance

An NRS Retention and Disposal Schedule was produced as an output of the information audit exercise completed in 2012-13. Key record types were identified along with their recommended minimum retention periods, in line with statutory and legislative obligations, as well as business need. The Retention and Disposal Schedule is mapped to the functional structure of the NRS Business Classification Scheme and also contains information relating to the recommended disposal procedure and the vital status of NRS records. It acts as a vital reference point for all staff when assessing how long they need to retain business information and will be actively used to review records held in legacy information systems.

In eRDM the retentions periods identified in the Scottish Government's Retention and Schedule are applied to files created within the system. The retention periods have been mapped to file types which are then used against the files used in eRDM. These standard retention rules are used by all of the Scottish Government and its non-ministerial departments and agencies.

At present retention rules are not being actively applied to shared drives and some line of business systems, but the next phase of the NRS EDRMS Project will address how information held in legacy storage and systems is reviewed and disposed of in line with the NRS Retention and Disposal Schedule.

Emails stored on the Exchange Server are subject to the retention periods defined in the Scottish Government's Email Archiving Policy. Information held on personal storage areas on network drives are subject to the retention periods defined in the Scottish Government's Archiving Policy for Shared Drives.

Evidence of Compliance

- Item 008: NRS Retention and Disposal Schedule
- Item 009: Scottish Government File Type Guidance
- Item 010: Scottish Government Casework File Type Guidance
- Item 011: Managing Email Policy (51KB PDF)
- Item 012: Scottish Government Email Archiving
- Item 013: Scottish Government Archiving Policy for Shared Drives
- Item 014: EDRMS Project Transition Strategy Scoping Document

Future Developments

The Scottish Government are pursuing a project to upgrade the current eRDM system and as part of this project will consider rationalising the current business classification scheme. As part of this review they will also assess their retention and disposal schedule to ensure it remains relevant. If changes are made to the file types used in eRDM the RMP will updated to reflect this. NRS Government Records Branch will work with the Records Manager to agree a selection policy for the NRS records held in the eRDM system.

Assessment and Review

The retention schedules used within NRS will be subject to ongoing monitoring and annual review to ensure they continue to identify all record types created in NRS and their appropriate retention periods.

Responsible Officer

Head of Records Management: John Simmons.

ELEMENT 6: DESTRUCTION ARRANGEMENTS

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 6: Destruction arrangements should evidence the arrangements that are in place for the secure destruction of confidential information. Clear destruction arrangements detailing the correct procedures to follow when destroying business information are necessary in order to minimise the risk of an information security incident and ensure that the organisation meets its obligations in relation to the effective management of its records, throughout their lifecycle.

Statement of Compliance

The Records Disposal Policy describes procedures for the disposal of information in NRS. All official paper waste is disposed of by confidential shredding. Secure consoles have been introduced to house all confidential paper waste until it is collected by a third party contractor. Electronic data selected for destruction is purged from disk backups after 12 weeks. Guidance on the correct procedures for the disposal of waste in all formats has been issued to staff and is available on the intranet.

Evidence of Compliance

- Item 015: Records Disposal Policy
- Item 008: Retention and Disposal Schedule
- Item 016: Shred-It Certification and certificates of destruction
- Item 017: SCOTS Back up and destruction procedures

Future Developments

There are no planned future developments.

Assessment and Review

The policy and disposal arrangements are subject to ongoing monitoring and annual review by the Information Security and Assurance Team and the Records Manager.

Responsible Officer:

Head of Information Security and Assurance: Mary Henderson.
Head of Records Management: John Simmons.

ELEMENT 7: ARCHIVING AND TRANSFER ARRANGEMENTS

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 7: 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 appropriate opportunity and the corporate memory of the organisation is fully and accurately preserved.

Statement of Compliance

NRS complies with the requirements for the review and transfer of records to public archives in the Section 61 Code of Practice: Records Management. Business areas within NRS transfer records of enduring value to the NRS archive. Government Records Branch has custodial responsibility for these archives under the management responsibility of the Deputy Keeper of the Records of Scotland. The NRS Archiving Arrangements Policy describes the agreed process for transferring records, in all formats, from operational records management systems to the NRS archive. The policy describes the roles of the records manager, information owners and Government Records Branch in this process, and the actions and activities that NRS staff must carry out to prepare records selected for transfer. When preparing born-digital records for transfer staff will follow the NRS Guidance for Depositors on the Transfer of Born Digital Records.

Evidence of Compliance

- Item 018: Archiving Arrangements Policy
- Item 019: Archive Service Accreditation award letter of Accredited Status
- Item 008: Retention and Disposal Schedule
- Item 015: Records Disposal Policy
- Item 020: GRO and SRO Fonds – Top Level Descriptions
- Item 021: Guidance for Depositors on the Transfer of Born Digital Records

Future Developments

NRS Government Records Branch will work with the Records Manager to agree a selection policy for the NRS records held in the eRDM system. New guidance for staff on how to sensitivity review records before transfer to archive will also be produced.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and will be reviewed annually or biennially.

Responsible Officer

Records Manager: John Simmons

Head of Government Records Branch: Bruno Longmore

ELEMENT 8: INFORMATION SECURITY

Introduction

A mandatory element of the Public Records (Scotland) Act 2011, Element 8: Information security must make provisions for the proper level of security of its records. There must be evidence of robust information security procedures that are well understood by all members of staff. 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.

Statement of Compliance

NRS has a number of well-established information security policies and procedures in place which all staff are required to comply with. These policies are approved by the Chief Executive and are reviewed on an annual basis. Information Security and Information Assurance in NRS is organised in line with the guidance and requirements in HMG Security Policy Framework and the National Cyber Security Centre guidance. All of these standards are closely aligned to the International Security standard: ISO/IEC 27001:2013. NRS complies with the security and access requirements of the Section 61 Code of Practice: Records Management.

Iron Mountain utilises electronic, physical and operational access controls at their facilities. They operate an Information Security Management System which complies with the requirements of ISO 27001.

Evidence of Compliance

- Item 022: Information Security Policy Statement
- Item 023: Information Assurance Policy Framework
- Item 024: Data Handling Policy
- Item 025: Information Assurance and Accreditation Policy
- Item 026: Security Incident Management Policy
- Item 027: Security Risk Management Policy
- Item 028: Continuity[2] Security and Resilience Overview
- Item 056: Access Control Policy Register

Evidence relating to records stored at Iron Mountain:

- Item 201: Iron Mountain ISO/IEC 27001:2005 Certificate
- Item 202: Iron Mountain Record Centre Security
- Item 203: A Compliant Records Management Solution for NRS
- Item 204: Iron Mountain Uk Ltd Vetting Policy & Procedure

Future Developments

The Information Security and Assurance Team are currently reviewing each of the policies to ensure that they are relevant to, and applied uniformly across, the whole organisation.

Assessment and Review

The policies are informally reviewed at least quarterly by the Information Assurance and Security Team and formally at least annually by the Business Leadership Group Team. The Keeper of the Records of Scotland will be informed if there are any changes to policies and procedures.

Responsible Officer

Head of Information Security and Assurance: Mary Henderson.

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

NRS 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. The NRS Data Protection Policy is a statement of public responsibility and demonstrates the organisation's commitment to compliance with the Act and the safeguarding and fair processing of all personal data held. Two supporting codes of practice have been drawn up to ensure NRS complies with the legislation by following organisation wide policies and procedures for the management of information created or received by us in the course of our business transactions. All staff undertake annual mandatory data protection training.

NRS follows an approach of privacy by design and uses privacy impact assessments (PIAs) for all projects which involve the handling of personal data and which may have an impact on privacy in order to help us identify the most effective way of complying with our data protection obligations and meeting individuals' expectations of privacy.

The Head of Records Management acts as Data Protection Officer and Freedom of Information Officer for NRS. The Privacy Group is responsible for considering privacy issues across programmes and projects, and for peer reviewing privacy impact assessments.

A notification for the Registrar General and the Keeper who are the data controllers for NRS has been submitted to the Information Commissioner for inclusion in the Data Protection Public Register.

Evidence of Compliance

- Registration number in the Data Protection Register is Z2886501
- Item 029: Data Protection Policy (208KB PDF)
- Item 030: Data Protection Code of Practice – Business Information (88KB PDF)
- Item 031: Data Protection Code of Practice – Archive Collections (397KB PDF)

Future Developments

NRS will be taking all necessary steps to ensure that it operates a level of data protection which is compliant with the EU General Data Protection Regulation, and any related UK data protection legislation, by May 2018.

Assessment and Review

The data protection policies and codes of practice are subject to ongoing monitoring and annual review to ensure they remain accurate and up to date. The data protection register entry is renewed annually and updated whenever there are any changes to the purposes for processing personal data.

Responsible Officers

Chief Executive of National Records of Scotland: Tim Ellis
Data Protection Officer: John Simmons.

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

This element was agreed in June 2013 on improvement terms. NRS now has business continuity arrangements in place to ensure that key systems and services can be recovered as soon as possible in the event of an incident. NRS has developed a series of related business continuity plans for sites and services which are integrated together within a Business Continuity Management System (BCMS). The business continuity plans were developed following a comprehensive business impact analysis (BIA) of all of NRS' functions and activities, which identified the resources needed to resume business operations within acceptable recovery timeframes. BIAs for each site document the vital records needed to restore business functions and their relative resilience or vulnerability.

NRS has developed ICT disaster recovery plans and procedures. Electronic data in NRS is backed up to disk on a 24 hour replication cycle, with instantaneous incremental backups and full backups every evening. Electronic files which have been deleted by users from devices will remain backed up for 12 weeks and 13 week old data is purged.

NRS has archives disaster planning procedures in place which are reviewed and updated at least annually, as well as a contract with a specialist disaster response company and informal arrangements with national bodies in the event of an emergency. The archives disaster recovery plan has also been incorporated into the BCMS.

Iron Mountain have business continuity plans for all their storage facilities. Location managers are responsible for ensuring that all issues of business continuity management are considered for their locations. Iron Mountain carry out at least four test exercises a year at sites within the UK and Europe.

Evidence of Compliance

- Item 032: NRS Business Continuity and Disaster Recover Arrangements
- Item 033: Disaster Plan (Hard Copy)
- Item 028: Continuity[2] Security and Resilience Overview

- Item 034: Continuity[2] User Guide
- Item 035: Cairnsmore House Business Continuity Plan
- Item 036: General Register House Business Continuity Plan
- Item 037: Ladywell House Business Continuity Plan
- Item 038: New Register House Business Continuity Plan
- Item 039: Thomas Thomson House Business Continuity Plan
- Item 040: West Register House Business Continuity Plan
- Item 041: NRS Emergency Plan
- Item 008: Retention and Disposal Schedule
- Item 042: eRDM Business Continuity Plan
- Item 060: NRS ICT Disaster Recovery Plan

Evidence relating to records stored at Iron Mountain:

- Item 208: Iron Mountain Business Continuity Plan Pro-forma
- Item 209: Iron Mountain Business Continuity Exercise Report
- Item 210: Iron Mountain Store Environmental Monitoring Readings

Future Developments

NRS will continue to develop its ICT disaster recovery capability to ensure that ICT services will be maintained or recovered in an efficient and prioritised manner to help safeguard the business continuity and reputation of National Records of Scotland.

Assessment and Review

Business continuity plans are reviewed and updated at least annually. BIAs are carried out when any new business processes are introduced or following any changes to the delivery of services. A BCMS management review will be carried out annually or in the event of major change within the organisation. Business continuity and contingency planning was subject to internal audit at the beginning March 2015 and arrangements continue to be audited annually by the NRS Audit and Risk Committee. NRS may seek peer review of its BC planning with other public sector organisations.

Responsible Officers

Chief Executive of National Records of Scotland: Tim Ellis.
Business Continuity Leader: Gerry Donnelly.

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

The Scottish Government's eRDM system, which NRS now uses to manage its corporate information, controls how users can create, edit, read, delete and apply restrictions to documents. It provides a full, unalterable audit trail of all actions taken upon documents, metadata or aggregations within the system.

An audit trail is maintained for the legacy registered paper files which are managed by the Records Management Unit and the access controls in operation within the statistical areas generate an access log for restricted data. The legacy SharePoint electronic document management system includes functionality which protects documents from changes, but a full audit trail is not available. Presently many documents stored on shared drives can be moved, edited, renamed and deleted without actions being auditable. The next phases of the EDRMS Project will seek to address these issues.

NRS also creates and manages considerable quantities of structured and semi-structured electronic data including: SAS (Statistical Analysis System) data sets; audio and visual media assets; GIS (Geo Spatial Information) maps and data sets; linked spreadsheets; and databases. All of this information is managed in compliance with relevant legislative and regulatory frameworks. Any corporate records generated from this data will be managed with reference to the NRS Retention and Disposal Schedule, with adequate audit trail information accurately captured.

NRS has also been working to improve how records are management in all environments by introducing new guidelines on document naming, use of version control, and the management of email.

NRS has semi-active records stored off site at Iron Mountain (IM). IM works to operating standards and procedures that are accredited to the quality assurance standard ISO 9001:2008. IM use their proprietary SafeKeeperPLUS system to manage all aspects of business records management. The system automates rigorous inventory control processes, manages records databases with sophisticated

indexing, processes all customer requests for filing and retrievals, and handles all billing and service information.

NRS uses the Iron Mountain Connect web-based portal to control how its records are stored, handled and retrieved. IM Connect provides designated users with the facility to retrieve records and return them to store and to generate activity and inventory reports which are used to monitor the storage and movement of records.

Evidence of Compliance

- Item 043: Scottish Government Audit Trail
- Item 044: Records Management Unit – User Manual
- Item 045: Document Naming and Control Guidelines (77KB PDF)
- Item 011: Managing Email Policy (51KB PDF)
- Item 046: Access Control Policy
- Item 047: EDRMS Project Portfolio Business Case

Evidence relating to records stored off site at Iron Mountain:

- Item 203: Iron Mountain: A Compliant Records Management Solution for NRS
- Item 205: Iron Mountain ISO 9001:2008 Certificate
- Item 206: Iron Mountain SafeKeeperPLUS workflows
- Item 207: Iron Mountain Connect data sheet

Future Developments

The Scottish Government are pursuing a project to upgrade the current eRDM system. Any upgrade will deliver the same audit trail functionality.

Assessment and Review

Progress on the successful implementation of eRDM within NRS will be monitored and reviewed by the EDRMS Project Board. The Keeper of the Records of Scotland will be kept informed of progress and changes.

Responsible Officers

Head of Records Management: John Simmons.
Director of ICT Operations: Sam Bedford.

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 clearly defined and made available within organisations so as 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

Core competencies, key knowledge and skills required by staff with responsibilities for records management have been clearly defined within a Records Management Competency Framework, ensuring that staff understand their roles and responsibilities and can offer expert advice and guidance. The Records Management Competency Framework has identified that the records manager will have a degree or postgraduate level qualification in information or records management.

Records management is identified as a distinct stream within the organisation's training portfolio and Corporate Development ensure that staff with specific records management responsibilities receive the training they require. Guidance is provided to all staff on induction and is available on the intranet. All staff receive training on how to use the Scottish Government's eRDM system. Additional training is provided to those staff that take on the Information Management Support Officer (IMSO) role and act as localised points of contact for records management and as gatekeepers of eRDM. Training presentations on records management have been developed which explain why records management is important and the arrangements for records management operated in NRS. Training is also delivered to meet particular staff needs identified by team leads in business areas.

Evidence of Compliance

- Item 003: Records Manager Job Summary (35KB PDF)
- Item 048: Records Management Competency Framework (43KB PDF)
- Item 049: Information Management Roles and Responsibilities in NRS (33KB PDF)
- Item 050: An Introduction to Records Management
- Item 051: Document and Records Management in NRS

Future Developments

Practical workshops focused on how teams can improve how they manage and access information will be run to meet business needs.

Assessment and Review

This competency framework will be reviewed annually by the records manager. The training programme will be reviewed annually by the records manager and corporate development manager.

Responsible Officer

Head of Records Management: John Simmons.
Organisational Development Manager: Wendy Ruddoch

ELEMENT 13: REVIEW AND ASSESSMENT

Introduction

Records Management practices in place within an organisation must remain fit for purpose. Procedures should be closely monitored, assessed and reviewed with a view to ensuring ongoing compliance and commitment to best practice recordkeeping. The Keeper expects the Records Management Plan to have in place mechanisms for regularly reviewing its contents in order to ensure processes are operating successfully and identifying processes which require modification.

Statement of Compliance

Each of the policies and procedures produced in line with the requirements of the Public Records (Scotland) Act 2011 has been prepared in consultation with colleagues across the organisation. Each new policy has been reviewed in detail in order to ensure compliance with all business as well as legal obligations.

Evidence of Compliance

Item 002: Records Management Policy (50KB PDF)

Future Developments

An Information Board was established in July 2016. The board will be responsible for reviewing and assessing the RMP, and the records management policies and practices within it, and will oversee the delivery of the records management programme.

Assessment and Review

All policies and procedures are subject to ongoing monitoring and annual or biennial review.

Responsible Officer

Head of Records Management: John Simmons.

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 what the disposal arrangements are.

Statement of Compliance

NRS exercises great care when sharing information. NRS follows the published guidance from HMG Cabinet Office and the principles of the International Security Standard ISO 27001, and adheres to the Information Commissioner's Data Sharing Code of Practice and the Guiding Principles for Data Linkage. Access control policies define access rights and security controls for personnel that need to use systems and access data within the organisation to perform their job function. Data sharing is carried out under transparent and proportionate controls and security processes. Data sharing agreements are used to record specific requirements for and the circumstances of information sharing, ensuring that data is shared fairly and lawfully. NRS maintains a central register of all data sharing and processing agreements. When undertaking any new data sharing activities which involve personal information a privacy impact assessment will be undertaken to ensure that any privacy risks are identified and mitigated. A secure extranet has been set up to enable NRS to share corporate information with external partners and stakeholders.

All staff receive information security and governance training on induction and undertake mandatory data protection training annually. Staff involved in data linkage activities are properly trained on data security policies and procedures, and undertake periodic refresher training.

Our Guide to Information describes information we routinely publish, while our Open Data Publishing Plan describes data that can be used and shared by anyone, for any purpose, without restriction and for free.

Evidence of Compliance

- Item 052: Statement on Information Sharing
- Item 053: Data Sharing Agreement template
- Item 054: Data Sharing Guidelines
- Item 055: Data Sharing and Processing Agreements Register
- Item 056: Data Sharing Agreement between Registrar General and Scottish Government Education Analytical Services
- Item 046: Access Control Policy

- Item 057: Access Control Policy Register
- Item 058: NRS Guide to Information
- Item 059: Open Data Publishing Plan

Future Developments

NRS will review its arrangements for information sharing to ensure they are compliant with the EU General Data Protection Regulation, and any related UK data protection legislation, by May 2018.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and to annual review.

Responsible Officer(s)

Head of Information Security and Assurance: Mary Henderson
Head of Records Management: John Simmons

ANNEX A: EVIDENCE SUBMITTED

Evidence of compliance within NRS			
Reference	**Document Name**	**Date**	**Elements**
Item 001	Statement of Responsibility for Records Management	Feb 2017	1, 2
Item 002	Records Management Policy	Jul 2016	1, 2, 3
Item 003	Records Manager Job Summary	Jan 2014	2, 12
Item 004	NRS Business Classification Scheme,	Jan 2013	4
Item 005	Scottish Government Business Classification Scheme	Jun 2015	4
Item 006	Scottish Government Fileplan Levels 1 to 3	Jun 2015	4
Item 007	Extract of NRS file in eRDM	Jul 2016	4
Item 008	NRS Retention and Disposal Schedule	Jan 2013	5, 6, 7, 10
Item 009	Scottish Government File Type Guidance	Jun 2015	5
Item 010	Scottish Government Casework File Type Guidance	Jun 2015	5
Item 011	Managing Email Policy	Jan 2015	5, 11
Item 012	Scottish Government Email Archiving	Apr 2015	5
Item 013	Scottish Government Archiving Policy for Shared Drives	Mar 2015	5
Item 014	EDRMS Project Transition Strategy – Scoping Document	Jul 2016	5
Item 015	Records Disposal Policy	Mar 2014	6, 7
Item 016/1	Certificate of Destruction – Shred-It	Feb 2013	6
Item 016/2	NAID-Europe Certificate awarded to Shred-It	2006	6
Item 016/3	Shred-It Waste Carriers Licence	2002	6
Item 016/4	Shred-It ISO 9001:2008 Certificate	2009	6
Item 016/5	Shred-It ISO 14001:2004 Certificate	2009	6
Item 016/6	British Security Industry Association Certificate of Membership, Shred-It	2005	6
Item 016/7	Duty of Care Audit	May 2011	6
Item 017	SCOTS Backup and Destruction Arrangements	Oct 2014	6
Item 018	Archiving Arrangements	Mar 2013	7
Item 019	Archives Accredited Status award letter	Nov 2014	7
Item 020	GRO and SRO Fonds Level Descriptions	Mar 2013	7
Item 021	Guidance for Depositors on the Transfer of Born Digital Records	Apr 2015	7
Item 022	Information Security Policy Statement	Sep 2016	8
Item 023	Information Assurance Policy Framework	Sep 2015	8
Item 024	Data Handling Policy	Aug 2015	8
Item 025	Information Assurance and Accreditation Policy	Nov 2013	8
Item 026	Security Incident Management Policy	Aug 2015	8
Item 027	Security Risk Management Policy	Aug 2015	8
Item 028	Continuity[2] Security and Resilience Overview	Aug 2014	8, 10
Item 029	Data Protection Policy	Mar 2016	9
Item 030	Data Protection Code of Practice – Archive Collections	Mar 2016	9
Item 031	Data Protection Code of Practice – Business Information	Jul 2016	9
Item 032	NRS Business Continuity and Disaster Recovery Arrangements	Oct 2014	10

Item 033	Disaster Plan (hard copy)	Mar 2013	10
Item 034	Continuity[2] User Guide	Mar 2015	10
Item 035	Cairnsmore House Business Continuity Plan	Jun 2015	10
Item 036	General Register House Business Continuity Plan	Jun 2015	10
Item 037	Ladywell House Business Continuity Plan	Jun 2015	10
Item 038	New Register House Business Continuity Plan	Jun 2015	10
Item 039	Thomas Thomson House Business Continuity Plan	Jun 2015	10
Item 040	West Register House Business Continuity Plan	Jun 2015	10
Item 041	NRS Emergency Plan	Apr 2015	10
Item 042	eRDM Business Continuity Plan	Aug 2013	10
Item 043	Scottish Government eRDM Audit Trail	Jan 2014	11
Item 044	Records Management Unit – User Manual	Mar 2014	11
Item 045	Document Naming Guidelines	Jun 2015	11
Item 046	Access Control Policy	Apr 2015	11, 14
Item 047	EDRMS Project Portfolio Business Case	Nov 2015	11
Item 048	Records Management Competency Framework	Jul 2016	12
Item 049	Information Management Roles and Responsibilities in NRS	Oct 2015	12
Item 050	An Introduction to Records Management	Mar 2015	12
Item 051	Document and Records Management in NRS	Jan 2016	12
Item 052	Statement on Information Sharing	Jan 2013	14
Item 053	Data Sharing Agreement template	Jun 2017	14
Item 054	Data Sharing Guidelines		
Item 055	Data Sharing and Processing Agreements Register	Apr 2017	14
Item 056	External Data Sharing Agreement between Registrar General and Scottish Government Education Analytical Services	Feb 2014	14
Item 057	Access Control Policy Register	Feb 2017	11, 14
Item 058	NRS Guide to Information	2014	14
Item 059	NRS Open Data Publishing Plan	2016	14
Item 060	NRS ICT Disaster Recovery Plan	Mar 2017	10

Evidence relating to records stored at Iron Mountain			
Reference	**Document Name**	**Date**	**Elements**
Item 201	Iron Mountain ISO/IEC 27001:2005 Certificate	Nov 2012	8
Item 202	Iron Mountain Record Centre Security	Feb 2014	8
Item 203	A Compliant Records Management Solution for NRS	Apr 2013	8, 11
Item 204	Iron Mountain Uk Ltd Vetting Policy & Procedure	Jan 2013	8
Item 205	Iron Mountain ISO 9001:2008 Certificate	Jan 2013	11
Item 206	Iron Mountain SafeKeeperPLUS workflows	Feb 2014	11
Item 207	Iron Mountain Connect data sheet	Feb 2012	11
Item 208	Iron Mountain Business Continuity Plan and Planning Location-Information Pro-forma	May 2012	10
Item 209	Iron Mountain Business Continuity Exercise Findings and Recommendations	Apr 2012	10
Item 210	Iron Mountain Store Environmental Monitoring Readings	Jul 2016	10