National Records of Scotland

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

May 2019

Document Control

Title	NRS Records Management Plan
Prepared By	Head of Information Governance
Approved Internally By	Director of Information and Record Services
Date of Approval	01 May 2019
Version Number	3.7
Review Frequency	Biannually
Next Review Date	October 2019

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
3.5	28 March 2018	Final	John Simmons	Change to data protection officer
3.6	24 July 2018	Final	John Simmons	To reflect staff changes
3.7	06 February 2019	Final	John Simmons	To reflect staff changes and recent developments

CONTENTS

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 non-ministerial offices of the Registrar General and the Keeper are separately named as authorities in the schedule of the Act. These offices are currently held by Paul Lowe, the Chief Executive of National Records of Scotland (NRS).

NRS is a non-ministerial department of the Scottish Government. Our purpose is to collect, preserve and produce information about Scotland's people and history and make it available to inform current and future generations. We were established on 1 April 2011, following the merger of the General Register Office for Scotland (GROS) and the National Archives of Scotland (NAS). For administrative purposes NRS sits within the Scottish Government’s Culture, Europe and External Affairs portfolio.

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.

Changes continue to be made to the content of the RMP as new corporate policies and procedures for the management of records are developed and existing ones reviewed and revised. The Keeper is regularly alerted to any significant changes in accordance with section 5(6) of the Act. The Chief Executive will be invited to resubmit the RMP for agreement by the Keeper during 2019.

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 Director of Information and Records Services: Laura Mitchell.

Evidence of Compliance

Primary evidence:

- Item 001: Statement of Responsibility for Records Management
- 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: Paul Lowe.

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 Information Governance: 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
- Item 002: Records Management Policy (158KB 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
Director of Information and Record Services: Laura Mitchell.

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.

Our Information Action Plan documents our strategic information aims and objectives, aligns these with our corporate plans and commitments, and provides a vehicle for documenting, co-ordinating, and monitoring the initiatives needed to deliver against those aims and objectives.

Evidence of Compliance

- Item 002: Records Management Policy (158KB PDF)
- Item 055: Information Action Plan

Future Developments

There are no planned future developments.

Assessment and Review

Our Records Management Policy is subject to ongoing monitoring and annual review to ensure that it continues to reflect the organisational position in relation to recordkeeping. Progress against our Information Action Plan will be reported to our Executive Management Board on biannual basis.

Responsible Officer

Head of Information Governance: 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
NRS manages its current records 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. The system was fully adopted by the organisation by March 2017.

NRS has developed and maintains an Information Asset Register (IAR) which captures all of the organisation's information assets. The IAR incorporates a record of processing activities for information assets involving personal data. Our information assets have been exported into a data landscape to enable analysis of our business architecture.

Evidence of Compliance
- Item 003: Scottish Government Business Classification Scheme
- Item 004: Scottish Government Fileplan Levels 1 to 3
- Item 005: Extract of NRS files in eRDM
- Item 006: Information Asset Register
- Item 056: Data Landscape

Future Developments
NRS may develop data models to help us better understand and exploit our information, its characteristics, flows and relationships.

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

Responsible Officer
Head of Information Governance: 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

The NRS Retention and Disposal Schedule identifies the record types created by the organisation and their recommended retention periods, in line with statutory and legislative obligations, as well as business need. Following the implementation of eRDM, the Retention Schedule was mapped to the topical structure of the Scottish Government Business Classification Scheme and updated to reflect the retention and disposal actions used within the eRDM system. The Retention Schedule identifies records which are vital to operations and also records of enduring value which should be preserved in the archives. It serves as a reference point for all staff when assessing how long they need to retain business information and is being actively used to review records held in legacy information systems.

As part of a continuing programme of work to improve the management of corporate information held in legacy systems, an extensive review of information stored on network shared drives was undertaken from October 2017 to April 2018. The review has enabled retention rules to be applied to all legacy corporate information stored on shared drives. Documents left on existing drives will be destroyed after 5 years; documents requiring longer retention for business purposes have been transferred to a new storage area with a 15 year retention; documents with enduring value have been transferred to another new storage area and will be transferred to archive in due course.

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.

Records involving personal data have been identified within both the Retention Schedule and also the record of processing activities incorporated within our Information Asset Register. Records involving personal data are managed in compliance with the data protection principles.

Evidence of Compliance

- Item 007: NRS Retention and Disposal Schedule
- Item 008: Scottish Government File Type Guidance
- Item 009: Scottish Government Casework File Type Guidance
- Item 010: Managing Email Policy
- Item 011: Scottish Government Email Archiving
- Item 012: Scottish Government Archiving Policy for Shared Drives
- Item 006: Information Asset Register
- Item 013: Shared Drives Review Report

Future Developments

Archives Depositor Liaison Branch will work with the Information Governance Team to agree a selection policy for NRS records held in the eRDM system.

Assessment and Review

The retention schedules used within NRS are 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 Information Governance: 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 are used 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 is issued to staff on induction and is available on the corporate intranet.

Evidence of Compliance

- Item 014: Records Disposal Policy
- Item 007: Retention and Disposal Schedule
- Item 015: Sample certificates of destruction
- Item 016: 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 Governance Team and IT Security Team.

Responsible Officer:

Head of Information Governance: John Simmons.
Head of IT Security: Gary Stewart.

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. The Government Records Team of our Archive Depositor Liaison 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 asset owners, and Archive Depositor Liaison 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 017: Archiving Arrangements Policy
- Item 018: Archive Service Accreditation award letter of Accredited Status
- Item 007: Retention and Disposal Schedule
- Item 014: Records Disposal Policy
- Item 019: GRO and SRO Fonds – Top Level Descriptions
- Item 020: Guidance for Depositors on the Transfer of Born Digital Records

Future Developments

Archives Depositor Liaison Branch will work with the Information Governance Team to agree a selection policy for 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
Head of Information Governance: John Simmons.
Head of Archive Depositor Liaison: 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.

NRS achieved Cyber Essentials Plus certification in October 2018, demonstrating our commitment to continuous security improvement and providing a level of external independent assurance that we are doing the right things to help protect our customers, the systems and services we deliver and the data we are trusted to hold.

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 021: Information Security Policy Statement
- Item 022: Information Assurance Policy Framework
- Item 023: Data Handling Policy
- Item 024: Information Assurance and Accreditation Policy
- Item 025: Security Incident Management Policy
- Item 026: Security Risk Management Policy
- Item 027: Access Control Policy Register
- Item 057: Cyber Essentials Plus Certificate

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

Following an organisational restructure, a new operating model for the management of information security, information risk, and information governance will be put in place.

Assessment and Review

The policies are informally reviewed at least quarterly by the IT Security Team and annually by the Executive Management Board. The Keeper of the Records of Scotland will be informed if there are any changes to policies and procedures.

Responsible Officer

Senior Information Risk Owner (SIRO): Linda Sinclair.

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 data protection law in relation to the management, processing and protection of personal data. This law includes the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Protection Act 2018 (DPA), which came into effect on 25 May 2018. The NRS Data Protection Policy is a statement of public responsibility and demonstrates the organisation's commitment to compliance with data protection law, and to the safeguarding and fair, lawful and transparent processing of all personal data held. 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.

The Registrar General and the Keeper are the data controllers for NRS and are registered in the Information Commissioner's Data Protection Public Register.

The Director of Information and Record Services is Data Protection Officer (DPO) for NRS. The appointment of DPO at director level signals our firm commitment to safeguarding people's personal data.

NRS maintains records of processing activities which are incorporated within our Information Asset Register.

NRS follows an approach of privacy by design and uses data protection impact assessments (DPIAs) 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.

A Privacy Group is responsible for considering privacy issues across programmes and projects, and for peer reviewing data protection impact assessments.

Evidence of Compliance
- Item 028: Data Protection Policy (208KB PDF)
- Item 006: Information Asset Register
- Item 029: Data protection guidance on corporate intranet

- Item 030: DPIA guidance
- Item 031: DPIA report template
- Item 032: Personal data breach reporting policy, procedures and guidance

Future Developments
NRS will extend the use of data protection impact assessments (DPIAs) to evaluate the adequacy of some existing systems and processes.

Assessment and Review
The data protection policy and related procedures and guidance are subject to ongoing monitoring and annual review to ensure they remain accurate and up to date.

Responsible Officers
Chief Executive of National Records of Scotland: Paul Lowe.
Data Protection Officer: Laura Mitchell.

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. 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.

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 033: NRS Business Continuity and Disaster Recovery Arrangements
- Item 034: Archival Disaster Recovery Plan (Hard Copy)
- Item 035: Building Business Continuity Plans
- Item 036: Business Impact Analysis
- Item 007: Retention and Disposal Schedule

- Item 037: eRDM Business Continuity Plan
- Item 038: 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. 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: Paul Lowe.
Business Continuity Leader: Anna Krakowska.

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.

Previously, many documents stored on shared drives could be moved, edited, renamed and deleted without actions being auditable. At the end of our review of legacy information stored on shared drives, these areas were locked down to read only access.

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 039: Scottish Government Audit Trail
- Item 040: Records Management Unit – User Manual
- Item 041: Document Naming and Control Guidelines
- Item 010: Managing Email Policy
- Item 042: Access Control Policy

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

No further developments are planned at this stage.

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 Information Governance: John Simmons.
Director of IT Services: 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 043: Records Management Competency Framework
- Item 044: Information Management Roles and Responsibilities in NRS (33KB PDF)
- Item 045: An Introduction to Records Management
- Item 046: eRDM training material

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 and training programme will be reviewed annually by the Information Governance and People Services teams.

Responsible Officer
Head of Information Governance: John Simmons.
Director of Information and Records Services: Laura Mitchell.

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.

Information Management Maturity Models were run at the end of 2017 to analyse the current and aspirational information management status of NRS against the Gartner Information Management Maturity Model.

A new governance structure was established within NRS in 2018. The Executive Management Board and Digital Strategy Board now oversee the management and use of information in NRS, ensuring that the appropriate corporate controls are in place and commissioning, approving and monitoring new, existing and revised information policies.

Evidence of Compliance
Item 002: Records Management Policy (50KB PDF)
Item 047: NRS Governance Boards Terms of Reference

Future Developments
A self-assessment of our records management services will be carried out in 2019 using the Archive and Records Management Services Quality Improvement Framework (ARMS).

Assessment and Review
All policies and procedures are subject to ongoing monitoring and annual or biennial review. The Executive Management Board is responsible for reviewing and assessing the RMP, and the records management policies and practices within it, and oversees the delivery of the records management programme.

Responsible Officer

Head of Information Governance: 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 data protection impact assessment will be undertaken to ensure that any privacy risks are identified and mitigated.

Objective Connect is used to provide secure, private workspaces for sharing and collaborating with external partners and customers. The solution is integrated with the eRDM system and enables synchronisation and version control of content, and security, control and audit of information shared externally.

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 048: Statement on Information Sharing
- Item 049: Data Sharing Agreement template
- Item 050: Data Sharing Guidelines

- Item 051: Data Sharing and Processing Agreements Register
- Item 052: Sample Data Sharing Agreement between Registrar General and Scottish Government Education Analytical Services
- Item 041: Access Control Policy
- Item 027: Access Control Policy Register
- Item 053: NRS Guide to Information
- Item 054: Open Data Publishing Plan

Future Developments

NRS will continue to monitor its arrangements for information sharing to ensure they are fit for purpose, and balance the beneficial use and protective safeguarding of our information assets.

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 Governance: John Simmons.
Senior Information Risk Owner (SIRO): Linda Sinclair.

ANNEX A: EVIDENCE SUBMITTED

Reference	Document Name	Supporting Elements
Item 001	Statement of Responsibility for Records Management	1, 2
Item 002	Records Management Policy	1, 2, 3
Item 003	Scottish Government Business Classification Scheme	4
Item 004	Scottish Government Fileplan Levels 1 to 3	4
Item 005	Extract of NRS file in eRDM	4
Item 006	Information Asset Register	4, 5, 9
Item 007	NRS Retention and Disposal Schedule	5, 6, 7, 10
Item 008	Scottish Government File Type Guidance	5
Item 009	Scottish Government Casework File Type Guidance	5
Item 010	Managing Email Policy	5, 11
Item 011	Scottish Government Email Archiving	5
Item 012	Scottish Government Archiving Policy for Shared Drives	5
Item 013	Shared Drives review Report	5
Item 014	Records Disposal Policy	6, 7
Item 015	Sample Certificates of Destructions	6
Item 016	SCOTS Backup and Destruction Arrangements	6
Item 017	Archiving Arrangements	7
Item 018	Archives Accredited Status award letter	7
Item 019	GRO and SRO Fonds Level Descriptions	7
Item 020	Guidance for Depositors on the Transfer of Born Digital Records	7
Item 021	Information Security Policy Statement	8
Item 022	Information Assurance Policy Framework	8
Item 023	Data Handling Policy	8
Item 024	Information Assurance and Accreditation Policy	8
Item 025	Security Incident Management Policy	8
Item 026	Security Risk Management Policy	8
Item 027	Access Control Policy Register	8, 11, 14
Item 028	Data Protection Policy	9
Item 029	Data protection guidance on corporate intranet	9
Item 030	DPIA guidance	9
Item 031	DPIA report template	9
Item 032	Personal data breach reporting policy, procedures and guidance	9
Item 033	NRS Business Continuity and Disaster Recovery Arrangements	10
Item 034	Archives Disaster Recovery Plan	10
Item 035	Building Business Continuity Plans	10
Item 036	Business Impact Analysis	10
Item 037	eRDM Business Continuity Plan	10
Item 038	ICT Disaster Recovery Plan	10
Item 039	Scottish Government eRDM Audit Trail	11
Item 040	Records Management Unit – User Manual	11
Item 041	Document Naming Guidelines	11
Item 042	Access Control Policy	
Item 043	Records Management Competency Framework	12
Item 044	Information Management Roles and Responsibilities in NRS	12
Item 045	An Introduction to Records Management	12

Item 046	eRDM training material	12
Item 047	NRS Governance Boards Terms of Reference	13
Item 048	Statement on Information Sharing	14
Item 049	Data Sharing Agreement template	14
Item 050	Data Sharing Guidelines	14
Item 051	Data Sharing and Processing Agreements Register	14
Item 041	Sample Data Sharing Agreement between Registrar General and Scottish Government Education Analytical Services	14
Item 052	Access Control Policy Register	11, 14
Item 053	NRS Guide to Information	14
Item 054	NRS Open Data Publishing Plan	14
Item 055	Information Action Plan	3
Item 056	Data Landscape	4
Item 057	Cyber Essentials Plus Certificate	8

Reference	**Document Name**	**Supporting Elements**
Item 201	Iron Mountain ISO/IEC 27001:2005 Certificate	8
Item 202	Iron Mountain Record Centre Security	8
Item 203	A Compliant Records Management Solution for NRS	8, 11
Item 204	Iron Mountain UK Ltd Vetting Policy & Procedure	8
Item 205	Iron Mountain ISO 9001:2008 Certificate	11
Item 206	Iron Mountain SafeKeeperPLUS workflows	11
Item 207	Iron Mountain Connect data sheet	11
Item 208	Iron Mountain Business Continuity Plan and Planning Location-Information Pro-forma	10
Item 209	Iron Mountain Business Continuity Exercise Findings and Recommendations	10
Item 210	Iron Mountain Store Environmental Monitoring Readings	10