National Records of Scotland

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

September 2020

Document Control

Title	NRS Records Management Plan
Prepared By	Head of Information Governance
Approved Internally By	Director of Information and Records Services
Date of Approval	28 September 2020
Version Number	3.0
Review Frequency	Annual
Next Review Date	September 2021

Status Control

Version	Date	Status	Prepared by	Reason for Amendment
1.0	10 May 2013	Final	John Simmons, Records Manager	2013 submission
2.0	8 March 2017	Final	John Simmons, Head of Records Management	Progress Update Review
3.0	28 September 2020	Final	John Simmons, Head of Information Governance	2020 submission

CONTENTS

Introduction

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

The Public Records (Scotland) Act 2011 (PRSA) obliges named authorities to prepare and implement a RMP setting out proper arrangements for the management of their public 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 office 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, Tourism and External Affairs portfolio.

Chronology

A combined RMP for the Registrar General and the Keeper was first submitted in April 2013 and agreed by the Keeper in June 2013. The RMP has been amended since then to reflect improvements in arrangements, and changes to our strategic approach and personnel. New corporate policies and procedures for the management of records have been developed and existing ones reviewed and revised. The Keeper has been regularly alerted to any significant changes in accordance with section 5(6) of the Act. An updated RMP was submitted for assessment under the mechanism of the Progress Update Review (PUR) in 2017, with an assessment report published by the Keeper on 5 July 2017.

Records covered by the RMP

Part 1, section 3(1) of the PRSA states that:

"In this Act "public records" in relation to an authority means –
(a) records created by or on behalf of the authority in carrying out its functions,
(b) records created by or on behalf of a contractor in carrying out the authority's functions,
(c) records created by any other person that have come into the possession of the authority or a contractor in carrying out the authority's functions."

The scope of this RMP therefore extends beyond NRS's corporate records to include those archival records in the Scottish national archives which have come into the

possession of the Keeper in carrying out this archival function, and the registration and census records created in exercise of the Registrar General's functions.

While the focus of the RMP is on documenting proper arrangements for the management of NRS's corporate business records throughout their lifecycle, it also seeks to evidence how we manage, preserve, and safeguard our historic record holdings.

Structure and contents

The structure of the Records Management Plan follows the Keeper's published Model Records Plan and has 15 Elements.

The 15 Elements are:

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
15. Public records created or held by third parties

Element 1: Senior management responsibility

An individual senior staff member is identified as holding corporate responsibility for records management.

Statement of Compliance

The senior manager who has overall responsibility for the management of National Records of Scotland's public records and for this Records Management Plan is Laura Mitchell, Director of Information and Records Services.

Evidence of Compliance

- Item 001: NRS Records Management Policy
- Item 002: Letter of endorsement from Director of Information and Records Services
- Item 003: NRS Governance Structure
- Item 004: NRS Organisational Chart

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

An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.

Statement of Compliance

The person who has operational responsibility for records management in NRS is John Simmons, Head of Information Governance. He is responsible for ensuring organisational compliance with the Records Management Plan, for the provision of records management services across all NRS sites, and for managing the contract for records that are stored off-site with Iron Mountain.

Evidence of Compliance

- Item 001: NRS Records Management Policy
- Item 003: NRS Governance Structure
- Item 005: NRS Records Management Competency Framework
- Item 006: Head of Information Governance Personal Learning Plan

Future Developments

There are no planned future developments.

Assessment and Review

Training and development needs are monitored and reviewed annually to ensure that post-holders with records management responsibilities have the necessary skills and experiences to carry out their tasks. This element will be reviewed as soon as there any changes in personnel.

Responsible Officer

Director of Information and Records Services: Laura Mitchell.

Element 3: Records management policy statement

The authority has an appropriate policy statement on records management.

Statement of Compliance

NRS recognises that the effective management of our records 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.

Since our Records Management Plan was last submitted for formal assessment in 2013, we have been pursuing a programme of work in order to deliver on our commitment to effective records management. We have concentrated the management of our corporate records within the Scottish Government's electronic document and records management system, eRDM, and we have reached the final stages of a project to consolidate the data previously maintained on legacy network domains within a single common operating platform on our NRScotland network.

Evidence of Compliance

- Item 001: NRS Records Management Policy

Future Developments

A current contract for off-site storage services runs to December 2020 and a procurement process will be undertaken to award a new contract in late 2020.

Assessment and Review

Our Records Management Policy is subject to ongoing monitoring and review to ensure that it continues to reflect the organisational position in relation to recordkeeping.

Responsible Officer

Head of Information Governance: John Simmons.

Element 4: Business classification

Records are known and are identified within a structure, ideally founded on function.

Statement of Compliance

NRS manages its current records within the Scottish Government's electronic document and records management system, 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. A major upgrade of the eRDM system was delivered in 2019 as part of an improvement programme to make it easier to manage information and store, locate and share documents. The improvements will enable us to meet our legal obligations and help make our organisation more open, capable and responsive.

NRS has developed and maintains an Information Asset Register (IAR) which captures all of the organisation's information assets. Details are recorded in the IAR when information assets are added, augmented, replaced, removed, or their risk profile changes. The IAR incorporates a record of processing activities for information assets involving personal data.

Evidence of Compliance

- Item 007: Scottish Government Business Classification Scheme
- Item 008: Scottish Government Fileplan Levels 1 to 3
- Item 009: Extract of NRS files in eRDM
- Item 010: eRDM Browser functionality handbook
- Item 011: NRS Information Asset Register
- Item 012: NRS Information Governance Checklist

Future Developments

Information Governance checks will be formally incorporated into our business case development process to ensure that any changes to or impacts on information assets are fully considered.

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

Records are retained and disposed of in accordance with the Retention Schedule.

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, alongside legacy retention documentation, to inform the review of 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 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.

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 011: NRS Information Asset Register
- Item 013: NRS Retention and Disposal Schedule
- Item 014: Scottish Government File Type Guidance
- Item 015: Scottish Government Casework File Type Guidance

- Item 016: eRDM Email Housekeeping Guidance
- Item 017: eRDM Email Housekeeping tips
- Item 018: Scottish Government Email Archiving Policy
- Item 019: NRS Shared Drives Review Guidance
- Item 020: NRS Shared Drives Review Report

Future Developments

A bespoke retention schedule is being developed to capture retention and disposal actions for data created, collected and processed during Scotland's Census 2021.

We intend to carry out further analysis and investigation of legacy data on the SCOTS network using an e-discovery tool in order to confirm that all records which merit preservation have been identified and that personal data is not retained for longer than it is required.

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

Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.

Statement of Compliance

Our 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 certified third party contractor.

Electronic data stored on the NRScotland network which is selected for destruction is purged from incremental and full backups on a rolling 12 week cycle. A further monthly full back up, which has been implemented to ensure data recovery, is retained for 12 months.

Data stored on the Scottish Government's SCOTS network is replicated across two data centres. Backups are kept for 4 weeks and then permanently deleted.

Guidance on the correct procedures for the disposal of waste in all formats is documented in the Records Disposal Policy and guidance on arrangements for the disposal of physical waste is available on the corporate intranet.

Evidence of Compliance

- Item 013: NRS Retention and Disposal Schedule
- Item 021: NRS Records Disposal Policy
- Item 022: NRS Guidance on physical waste disposal arrangements
- Item 023: Sample certificates of destruction
- Item 024: Restore Datashred overview and on-site shredding factsheets
- Item 025: iTECS terms of supply
- Item 026: NRScotland Backup Procedure

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.
Director of IT Services: Laura Lucas.

Element 7: Archiving and transfer arrangements

Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'

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 Deputy Keeper of the Records of Scotland has management responsibility for these archival records and exercises this through our Archive Depositor Liaison Branch. NRS recently developed a new Memorandum of Understanding for transfer of records. An internal version of this MOU has been agreed between NRS Information Governance and Archive Depositor Liaison.

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. All NRS websites have been selected for preservation as part of the NRS Web Continuity Service: https://webarchive.nrscotland.gov.uk/

NRS is also responsible for the archival management of public records in the Scottish national archives which have come into the possession of the Keeper in carrying out their archival function. These comprise archival records collections that were gifted by or purchased from depositors, as well as 'orphan' records for which the Keeper has assumed responsibility when the record creator became defunct and no successor could be identified. Some records have been transferred to other archives under the Keeper's charge and superintendence in order to improve arrangements for access or preservation. For example, some records of local interest have been transferred to local archives.

NRS's archive service was awarded UK Archive Service Accreditation in 2014.

Evidence of Compliance

- Item 013: NRS Retention and Disposal Schedule
- Item 021: NRS Records Disposal Policy

- Item 027: NRS Archiving Arrangements Policy
- Item 028: NRS internal MOU on transfer of archives
- Item 029: NRS Archive Service Accreditation award letter of Accredited Status
- Item 030: NRS Guidance for Depositors on the Transfer of Born Digital Records
- Item 031: NRS Archive Collections - GRO and SRO Collections - Fonds Level Descriptions
- Item 032: NRS Archive Collections - Gifted and Purchased Collections – Fonds Level List
- Item 033: Example charge and superintendence agreement – between Keeper and Highland Council for Cameron-Head of Inverailort Collection

Future Developments

NRS will be reapplying for Archive Service Accreditation in 2020.

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

Records are held in accordance with information security compliance requirements.

Statement of Compliance

NRS has information security policies and procedures in place that are closely aligned to the international standard for information security management, ISO/IEC 27001:2013. We also comply with the security and access requirements of the Section 61 Code of Practice: Records Management. Information risks are captured and managed in our Corporate Risk Register, helping ensure that we apply appropriate controls to safeguard information and protect the interests of our stakeholders, while delivering objectives and making the most of opportunities.

NRS complies with the HMG Minimum Standard for Cyber Security and the Scottish Government Cyber Resilience Framework, and compliance with and certification to Cyber Essentials Plus is in place. Our Technical Security Standard defines security requirements for systems and services to ensure they are compliant with these standards.

All employees are subject to pre-employment screening checks, security cleared to the Baseline Personnel Security Standard, and undertake security awareness and data protection training.

Government Security Classifications are applied to documents stored in eRDM and group and user permissions are used to control access at both document and folder level. Access Controls Policies defining access rights and security controls are applied to any storage area or system where sensitive or protectively marked data is held. A security model has been implemented on the NRScotland network to ensure that data involving personal information is segregated and safeguarded.

Incident reporting arrangements are in place for security incidents and personal data breaches and post-incident reviews are carried out.

Iron Mountain utilise digital, 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 034: NRS Technical Security Standard
- Item 035: NRS Government Security Classifications guidance
- Item 036: NRS Security Incident Management Policy
- Item 037: NRS Personal data breach reporting policy, procedures and guidance

- Item 038: NRS Access Control Policy
- Item 039: NRS Access Control Policy Register
- Item 040: NRS Cyber Essentials Plus Certificate
- Item 041: eRDM IMSO Handbook
- Item 042: NRS Clear Desk Policy
- Item 043: NRS Working from home guidelines
- Item 044: Scottish Government IT Code of Conduct
- Item 045: NRS Corporate Risk Register

Evidence relating to records stored at Iron Mountain

- Item 101: Service Proposal for Compliant Records Management Solution
- Item 102: ISO/IEC 27001:2005 Certificate
- Item 103: Iron Mountain Record Centre Security
- Item 104: Iron Mountain Vetting Policy and Procedure

Future Developments

NRS IT Security is looking to deliver improvements to all aspects of IT security within NRS, including a project to implement an Identity and Access Management system to replace our existing access control arrangements.

Assessment and Review

Information security policies will be reviewed annually by the Security Working Group. Spot checks of the classification of documents stored in eRDM are carried out monthly. Access control policies are reviewed annually by Information Asset Owners and regularly audited by Information Governance. The Keeper of the Records of Scotland will be informed if there are any changes to policies and procedures.

Responsible Officer

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

Element 9: Data protection

Records involving personal data are managed in compliance with data protection law.

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 Records 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. The DPO and Head of Information Governance hold GDPR practitioner certificates.

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 and activities which involve the handling of personal data and which may have an impact on privacy. We do this 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, projects and business as usual, and for peer reviewing data protection impact assessments.

Evidence of Compliance

- Item 011: NRS Information Asset Register

- Item 037: NRS Personal data breach reporting policy, procedures and guidance
- Item 046: NRS Data Protection Policy
- Item 047: NRS Data Protection Impact Assessment (DPIA) policy and guidance
- Item 048: NRS Data Protection Impact Assessment (DPIA) report template
- Item 049: NRS example DPIA
- Item 050: NRS Data protection guidance on corporate intranet
- Item 051: NRS Privacy Notice
- Item 052: NRS Registration Privacy Notice
- Item 053: NRS Records Reclosure and Takedown Policy
- Item 054: NRS Data Sharing and Processing Agreements Register
- Item 055: NRS Data Sharing Agreement template
- Item 056: Data protection e-learning
- Item 057: NRS Privacy Group Terms of Reference

Future Developments

NRS is extending the use of data protection impact assessments (DPIAs) to evaluate the adequacy of established 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

Record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.

Statement of Compliance

NRS 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. A series of related business continuity plans for sites and services have been prepared. The business continuity plans were developed following a comprehensive business impact analysis (BIA) of all of NRS's 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 also developed ICT disaster recovery planning and procedures for our NRScotland network. We have recently been reviewing service criticalities and are in the process finalising runbooks to assist with service recovery.

Electronic data stored on the network is backed up with incremental and full backups on a rolling 12 week cycle. A further monthly full back up, which is retained for 12 months, has now been implemented to ensure data recovery. Daily incremental backups are run on the Scottish Government's SCOTS network and full back ups are taken of the system at the weekend. Backups are kept for 4 weeks.

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 Scottish Council on Archives has collaborated with NRS to develop 'Planning Matters', a new suite of emergency planning guidance and templates for use by archives, and we will utilise these for our own response procedures.

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.

COVID-19 has presented NRS with new challenges and tested our resilience, but has also helped us improve our processes for incident control. The Incident Management Team has led an effective response and we have developed new guidance and support mechanisms as we adapt to remote working. The majority of employees have now signed up to receive alerts from our emergency messaging system, which allows us to communicate outwith our usual work communication

channels. Our home working arrangements have proved robust, our digital recordkeeping has not been disrupted, and we have been able to continue to deliver the majority of our services. While the closure of our buildings to limit the spread of the coronavirus has restricted access to the public registers and the public records stored in our archives, these records remain safeguarded and accessible where the need is urgent.

Evidence of Compliance

- Item 013: NRS Retention and Disposal Schedule
- Item 025: iTECS terms of supply
- Item 058: NRS Business Continuity Plans – October 2018
- Item 059: NRS Business Continuity Plan – September 2020
- Item 060: NRS Crisis Management Plans – September 2019
- Item 061: NRS COVID-19 Incident Management Team Handbook
- Item 062: NRS COVID-19 Archives Incident Response Control Protocol
- Item 063: SCA and NRS Planning Matters guidance and templates
- Item 064: Harwell Priority User Service
- Item 065: NRScotland runbooks and service criticalities overview
- Item 066: eRDM Business Continuity Plan

Evidence relating to records stored at Iron Mountain

- Item 107: Iron Mountain Business Continuity Plan Example
- Item 109: Iron Mountain Store Environmental Monitoring Readings

Future Developments

We are continuing to improve our business continuity planning and are in the process of finalising a new Business Continuity Plan and a series of related crisis plans for each of our sites, which are included as evidence.

On our NRScotland network, we aim to have implemented automated recovery of systems which support critical services by the end of 2020. Early in 2021 the NRS server estate will move from its current locations to two purpose built data centres. These will deliver improved security, environmental conditions and network resilience. A revised policy for testing and reviewing disaster recovery preparedness will then be developed for this platform.

Assessment and Review

Business continuity documentation will be 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.

Responsible Officers

Chief Executive of National Records of Scotland: Paul Lowe.
Head of Strategy and Planning: Anna Krakowska

Element 11: Audit trail: tracking and version control

The location of records is known and changes recorded.

Statement of Compliance

The Scottish Government's eRDM system, which NRS 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. A related audit trail is also created for information which is shared externally through the eRDM Connect platform.

An audit trail is maintained for the legacy paper file records management system, while legacy documents stored in the SharePoint electronic document management system are protected from changes. 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 significant 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. Access control policies are used to control access to this data. All information is managed in compliance with relevant legislative and regulatory frameworks. Any corporate records generated from this data are managed with reference to the NRS Retention and Disposal Schedule, with adequate audit trail information accurately captured.

We have improved how records are managed in all environments by introducing guidelines on document naming, use of version control, and the management of email.

NRS has semi-active records stored off-site at Iron Mountain. Iron Mountain works to operating standards and procedures that are accredited to the quality assurance standard ISO 9001:2008. Iron Mountain 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. Iron Mountain 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.

NRS tracks the location and movement our archival records using in-house records location, transmissions and ordering systems.

Evidence of Compliance

- Item 010: eRDM Browser functionality handbook
- Item 016: eRDM Email Housekeeping Guidance
- Item 017: eRDM Email Housekeeping tips
- Item 038: NRS Access Control Policy
- Item 067: eRDM Audit Trail
- Item 068: eRDM Connect Audit Trail
- Item 069: NRS Legacy Paper Records Management System Audit Trail
- Item 070: NRS Document Naming and Control Guidelines
- Item 071: NRS Document Naming – Use of acronyms and abbreviations
- Item 072: NRS Access Control Policy example

Evidence relating to records stored off-site at Iron Mountain

- Item 101: Iron Mountain Service Proposal for Compliant Records Management Solution
- Item 105: Iron Mountain Retrieval and Collection Workflows
- Item 106: Iron Mountain Connect Data Sheet
- Item 108: Iron Mountain Management Information Report
- Item 110: Iron Mountain Contract Variation Agreement

Future Developments

Data Protection Impact Assessments are carried out for new systems involving the processing of personal data.

Assessment and Review

We will continue to monitor use of eRDM and other information management systems to ensure they remain fit for purpose.

Responsible Officers

Head of Information Governance: John Simmons.
Director of IT Services: Laura Lucas.

Element 12: Records management training for staff

Staff creating, or otherwise processing records, are appropriately trained and supported.

Statement of Compliance

The core competencies, key knowledge and skills required by staff with responsibilities for records management have been clearly defined within a Records Management Competency Framework, which ensures that staff understand their roles and responsibilities and can offer expert advice and guidance. The Records Management Competency Framework has identified that the person designated records manager will have a degree or postgraduate level qualification in information or records management. Our People Services ensure that staff with specific records management responsibilities receive the training they require.

Guidance on records management is provided to all staff on induction and a series of guidance pages are available on the intranet. All staff also receive training on how to use the Scottish Government's eRDM system. To support the release of the latest version of eRDM a suite of online training modules and webinars were developed and tailored based on feedback from users. The new training allows users to access guidance material at a time and place suitable to them.

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.

The Information Governance Team provide support and deliver training to meet particular staff or team needs. This include refresher sessions on how to get the most out of eRDM and guidance on how to apply records management principles to the creation, maintenance and disposal of business information.

All staff undertake annual mandatory data protection training and new security awareness training is currently being introduced.

Evidence of Compliance

- Item 005: NRS Records Management Competency Framework
- Item 056: Data protection e-learning
- Item 073: Information Management Roles and Responsibilities in NRS
- Item 074: NRS guidance pages on records management and information governance on Connect intranet
- Item 075: eRDM training material

- Item 076: NRS Induction Welcome Pack

Future Developments

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

Assessment and Review

Completion of mandatory training is monitored. The competency framework and training requirements will be reviewed annually by the Information Governance and People Services teams.

Responsible Officers

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

Element 13: Assessment and review

Records Management arrangements are regularly and systematically reviewed with actions taken when required.

Statement of Compliance

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

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.

NRS has carried out periodic self-assessments of its information management maturity. Most recently a self-assessment was conducted in February 2020 with the Scottish Government's Analytical Data Management Team using their Data Management Maturity Model. These assessments have provided confidence in our levels of information management maturity, while also helping to identify areas for further improvement. A scheduled self-evaluation using the Scottish Council on Archives' Archive and Records Management Services Quality Improvement Framework (ARMS) has had to be postponed until later in 2020 in order to prioritise work on COVID-19 related activities.

Evidence of Compliance

- Item 001: Records Management Policy
- Item 077: NRS Governance Boards Terms of Reference
- Item 078: Data Management Maturity Model Assessment

Future Developments

A self-assessment of our records management services will be carried out later in 2020, following the completion of our network consolidation project, using the ARMS Framework.

Assessment and Review

All policies and procedures are subject to ongoing monitoring and annual or biennial review. The Executive Management Board oversees the delivery of the records management programme.

Responsible Officers

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

Element 14: Shared information

Information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.

Statement of Compliance

NRS exercises great care when sharing information. We follow the Information Commissioner's guidance on data sharing and the Scottish Government's Guiding Principles for Data Linkage. Data sharing is carried out using transparent and proportionate controls and robust security processes. Data sharing agreements are used to record the specific requirements and circumstances of information sharing, and ensure 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 usually be undertaken to ensure that any privacy risks are identified and mitigated.

NRS facilitates data access for ethically sound research which is in the public good and improves our understanding of equalities. Research applications to access census and health data are reviewed internally by the NRS Privacy Group and externally by the Statistics Public Benefit and Privacy Panel and the Public Benefit and Privacy Panel on Health and Social Care respectively. Secure and controlled access to census datasets is provided within the National Safe Haven, developed by the Edinburgh Parallel Computing Centre and administered by eDRIS (Public Health Scotland).

eRDM Connect is used to provide secure, private workspaces for sharing information 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.

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 054: NRS Data Sharing and Processing Agreements Register
- Item 055: NRS Data Sharing Agreement template
- Item 057: NRS Privacy Group Terms of Reference
- Item 079: NRS Data Sharing Guidelines
- Item 080: Example Data Sharing Agreement

- Item 081: NRS Guide to Information
- Item 082: NRS Open Data Publishing Plan
- Item 083: NRS Privacy Group Proportionate Assessment Form
- Item 084: Statistics Public Benefit and Privacy Panel Terms of Reference
- Item 085: Statistics Public Benefit and Privacy Panel Membership

Future Developments

NRS is pursuing a project to develop a new file transfer tool for internal and external data sharing that will meet our current and future requirements for sharing information.

We are also exploring how we can improve research access to our data through Research Data Scotland, which is developing a new model for how de-identified data can be brought together for public good research.

Assessment and Review

The policies and procedures under this element are subject to ongoing monitoring and to annual review. We will continue to monitor arrangements for information sharing to ensure they remain fit for purpose, and balance beneficial use with protective safeguarding.

Responsible Officers

Head of Information Governance: John Simmons.
Chief Executive: Paul Lowe.

Element 15: Public records created or held by third parties

Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.

Statement of Compliance

NRS has not tasked any third parties to carry out its functions. While NRS makes use of contractors and suppliers to help deliver services, these third parties operate to the direction and instruction of the Registrar General and the Keeper. All public records created as part of this service delivery are held by NRS.

Future Developments

No future developments are planned.

Assessment and Review

This element will be reviewed annually..

Responsible Officer

Chief Executive of National Records of Scotland: Paul Lowe.

ANNEX A: EVIDENCE SUBMITTED

Evidence relating to NRS records management arrangements

Reference	Document Name	Supporting Elements
Item 001	NRS Records Management Policy	1, 2, 3, 13
Item 002	Letter of endorsement from Director of Information and Records Services	1
Item 003	NRS Governance Structure	1, 2
Item 004	NRS Organisational Chart	1
Item 005	NRS Records Management Competency Framework	2, 12
Item 006	Head of Information Governance Personal Learning Plan	2
Item 007	Scottish Government Business Classification Scheme	4, 7, 10
Item 008	Scottish Government Fileplan Levels 1 to 3	4
Item 009	Extract of NRS files in eRDM	4
Item 010	eRDM Browser functionality handbook	4, 11
Item 011	NRS Information Asset Register	4, 5, 9
Item 012	NRS Information Governance Checklist	4
Item 013	NRS Retention and Disposal Schedule	5, 6, 7, 10
Item 014	Scottish Government File Type Guidance	5
Item 015	Scottish Government Casework File Type Guidance	5
Item 016	eRDM Email Housekeeping Guidance	5, 11
Item 017	eRDM Email Housekeeping tips	5, 11
Item 018	Scottish Government Email Archiving Policy	5
Item 019	Shared Drives Review Guidance	5
Item 020	Shared Drives Review Report	5
Item 021	Records Disposal Policy	6, 7
Item 022	NRS Guidance on physical waste disposal arrangements	6
Item 023	Sample certificates of destruction	6
Item 024	Restore Datashred overview and on-site shredding factsheets	
Item 025	iTECS terms of supply	6, 10
Item 026	NRScotland Backup Procedure	6
Item 027	NRS Archiving Arrangements Policy	7
Item 028	NRS internal MOU on transfer of archives	7
Item 029	Archive Service Accreditation award letter of Accredited Status	7
Item 030	NRS Guidance for Depositors on the Transfer of Born Digital Records	7
Item 031	NRS Archive Collections - GRO and SRO Collections - Fonds Level Descriptions	7
Item 032	NRS Archive Collections - Gifted and Purchased Collections Fonds – Fonds Level List	7
Item 033	Example charge and superintendence agreement – between Keeper and Highland Council for Cameron-Head of Inverailort Collection	7
Item 034	NRS Technical Security Standard	8
Item 035	NRS Government Security Classifications guidance	8
Item 036	NRS Security Incident Management Policy	8

Item 037	NRS Personal data breach reporting policy, procedures and guidance	8, 9
Item 038	NRS Access Control Policy	8, 11
Item 039	NRS Access Control Policy Register	8
Item 040	NRS Cyber Essentials Plus Certificate	8
Item 041	eRDM IMSO Handbook	8
Item 042	NRS Clear desk guidance	8
Item 043	NRS Working from home guidelines	8
Item 044	IT Code of Conduct	8
Item 045	NRS Corporate Risk Register	8
Item 046	NRS Data Protection Policy	9
Item 047	NRS Data Protection Impact Assessment (DPIA) policy and guidance	9
Item 048	NRS Data Protection Impact Assessment (DPIA) report template	9
Item 049	NRS example Data Protection Impact Assessment	9
Item 050	NRS Data protection guidance on corporate intranet	9
Item 051	NRS Privacy Notice	9
Item 052	NRS Registration Privacy Notice	9
Item 053	NRS Records Reclosure and Takedown Policy	9
Item 054	NRS Data Sharing and Processing Agreements Register	9, 14
Item 055	NRS Data Sharing Agreement template	9, 14
Item 056	Data protection e-learning	9, 12
Item 057	NRS Privacy Group Terms of Reference	9, 14
Item 058	NRS Business Continuity Plans – October 2018	10
Item 059	NRS Business Continuity Plan – September 2020	10
Item 060	NRS Crisis Management Plans – September 2019	10
Item 061	NRS COVID-19 Incident Management Team Handbook and overview	10
Item 062	NRS COVID-19 Archives Incident Response Control Protocol	10
Item 063	SCA and NRS Planning Matters guidance and templates	10
Item 064	Harwell Priority User Service	
Item 065	NRScotland runbooks and service criticalities overview	10
Item 066	eRDM Business Continuity Plan	10
Item 067	eRDM Audit Trail	11
Item 068	eRDM Connect Audit Trail	11
Item 069	NRS Legacy Paper Records Management Unit Audit Trail	11
Item 070	NRS Document Naming and Control Guidelines	11
Item 071	NRS Document Naming – Use of acronyms and abbreviations	11
Item 072	NRS Access Control Policy example	11
Item 073	Information Management Roles and Responsibilities in NRS	12
Item 074	NRS records management and information governance guidance pages on Connect intranet	12
Item 075	eRDM training material	12
Item 076	NRS Induction Welcome Pack	12
Item 077	NRS Governance Boards Terms of Reference	13
Item 078	Data Management Maturity Model Assessment	13
Item 079	NRS Data Sharing Guidelines	14
Item 080	NRS Example Data Sharing Agreement	14
Item 081	NRS Guide to Information	14

Item 082	NRS Open Data Publishing Plan	14
Item 083	NRS Privacy Group Proportionate Assessment Form	14
Item 084	Statistics Public Benefit and Privacy Panel Terms of Reference	14
Item 085	Statistics Public Benefit and Privacy Panel membership	14

Evidence relating to records stored off-site at Iron Mountain

Reference	Document Name	Supporting Elements
Item 101	Service Proposal for Compliant Records Management Solution for NRS	8, 11
Item 102	Iron Mountain ISO/IEC 27001:2005 Certificate	8
Item 103	Iron Mountain Record Centre Security	8
Item 104	Iron Mountain Vetting Policy and Procedure	8
Item 105	Iron Mountain Retrieval and Collection Workflows	11
Item 106	Iron Mountain Connect Data Sheet	11
Item 107	Iron Mountain Business Continuity Plan Example	10
Item 108	Iron Mountain Management Information Report	11
Item 109	Iron Mountain Store Environmental Monitoring Readings	10
Item 110	Iron Mountain Contract Variation Agreement	11