

Public Records (Scotland) Act 2011

**Keeper of the Records of Scotland
and Registrar General of Births, Deaths and Marriages for Scotland**

The Keeper of the Records of Scotland

13th January 2021

Contents

1. Public Records (Scotland) Act 2011	3
2. Executive Summary	4
3. Authority Background	4
4. Assessment Process	5
5. Model Plan Elements: Checklist	6
6. Keeper's Summary	32
7. Keeper's Determination	32
8. Keeper's Endorsement	33

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came fully into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor record keeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Executive Summary

This report sets out the findings of the Keeper's assessment of the RMP of the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 29th May 2020.

The assessment considered whether the RMP of the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland was developed with proper regard to the 14 elements of the Keeper's statutory Model Records Management Plan (the Model Plan) under section 8(3) of the Act, and whether in this respect it complies with it and the specific requirements of the Act.

The outcome of the assessment and the Keeper's decision on whether the RMP of the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

The Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland are two separate non-ministerial offices currently held jointly by Paul Lowe, Chief Executive of the National Records of Scotland (NRS).

NRS is a Non-Ministerial Department of the Scottish Government. Their purpose is to collect, preserve and produce information about Scotland's people and history and make it available to inform current and future generations. NRS was 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 they sit within the Scottish Government's Economy, Fair Work and Culture portfolio.

As the Keeper of the Records of Scotland, Mr Lowe is also responsible for implementing the Public Records (Scotland) Act 2011.

www.nrscotland.gov.uk

4. Keeper’s Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether the Keeper of the Records of Scotland and the Registrar General for Births Deaths and Marriages in Scotland’s RMP was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

G	The Keeper agrees this element of an authority’s plan.		A	The Keeper agrees this element of an authority’s plan as an ‘improvement model’. This means that he is convinced of the authority’s commitment to closing a gap in provision. He will request that he is updated as work on this element progresses.		R	There is a serious gap in provision for this element with no clear explanation of how this will be addressed. The Keeper may choose to return the RMP on this basis.
----------	--	--	----------	--	--	----------	--

5. Model Plan Elements: Checklist

Keeper of the Records of Scotland and Registrar General of Births Deaths and Marriages for Scotland (for simplicity the separate authorities will be referred to as 'NRS' in the assessment below)

Element	Present	Evidence	Notes
1. Senior Officer	G	G	<p>The Public Records (Scotland) Act 2011 (the Act) requires that an individual senior staff member is identified as holding corporate responsibility for records management in a public authority.</p> <p>Keeper of the Records of Scotland and Registrar General of Births Deaths and Marriages for Scotland (NRS) have identified Laura Mitchell, Director of Information and Records Services as the individual with overall responsibility for records management in the organisation.</p> <p>The identification of the Director of Information and Records Services to this role is supported by a <i>Covering Letter</i> from Ms Mitchell (see under General Comments below) and by the <i>Records Management Policy</i>, for example section 6.2.</p> <p>The Director of Information and Records Services is the NRS Data Protection Officer (see element 9).</p> <p>The Director of Information and Records Services approved the <i>Records Management Plan</i> (the <i>RMP</i>).</p>

			<p>The Director of Information and Records Services also approved the <i>Records Management Policy</i> (see element 3), the <i>Records Management Competency Framework</i>, the <i>Records Disposal Policy</i> (see element 6), the <i>Archiving Arrangements</i> document (see element 7), the <i>Depositor Guidance for the Transfer of Archival Born Digital Records and Access Control Policy NRS Digital Repository</i>, the <i>Clear Desk Guidance</i> document (see element 8), the <i>Data Protection Policy</i>, the <i>NRS Privacy Group Terms of Reference</i>, the <i>Data Protection Impact Assessment (DPIA) Policy and Guidance</i> and the <i>Personal Data Breach Reporting: Procedure and Guidance</i> (for all see element 9), the <i>Document Naming and Control Guidelines</i> (see element 11), the <i>Data Sharing Guidelines</i> (see element 14).</p> <p>It is clear from the above that the Director of Information and Records Services is closely aware of the records management provision in NRS.</p> <p>The Keeper agrees that NRS have identified an appropriate individual to this role as required by the Public Records (Scotland) Act (the Act).</p>
2. Records Manager	G	G	<p>The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.</p> <p>NRS have identified John Simmons, Head of Information Governance as the individual with day-to-day responsibility for implementing the RMP.</p> <p>The identification of the Head of Information Governance to this role is supported by a <i>Covering Letter</i> from Ms Mitchell (see element 1) and by the <i>Records Management Policy</i>, for example section 6.7.</p> <p>It is also supported by the <i>Information Management Roles and Responsibilities in NRS</i> document provided to the Keeper and by the <i>Personal Learning Plan Head of</i></p>

			<p><i>Information Governance</i> (also supplied).</p> <p>The Head of Information Governance prepared the <i>RMP</i>.</p> <p>The Head of Information Governance also prepared the <i>Records Management Policy</i> (see element 3), the <i>Records Management Competency Framework</i>, the <i>Records Disposal Policy</i> (see element 6), the <i>Archiving Arrangements</i> document (see element 7), the <i>Clear Desk Guidance</i> document (see element 8), the <i>Data Protection Policy</i>, the <i>NRS Privacy Group Terms of Reference</i>, the <i>Data Protection Impact Assessment (DPIA) Policy and Guidance</i> and the <i>Personal Data Breach Reporting: Procedure and Guidance</i> (for all see element 9) the <i>Document Naming and Control Guidelines</i> (see element 11) the <i>Data Sharing Guidelines</i> (see element 14).</p> <p>The Head of Information Governance also authorised the <i>NRS Retention Schedule</i> (see element 5) and the sample <i>Business Continuity Plans</i> received by the Keeper (see element 10).</p> <p>It is clear from the above that the identified individual has a detailed knowledge of the records management provision in the authority.</p> <p>The Head of Information Governance is responsible for liaising with Information Asset Owners around Freedom of Information Requests (see Local Records Management under General Comments below).</p> <p>In the evidence documents the Head of Information Governance is occasionally referred to as 'Corporate Records Manager' (for example <i>Archive Arrangements</i> document – see element 7 – section 3).</p> <p>The Head of Information Governance chairs the <i>NRS Privacy group</i> (see element</p>
--	--	--	--

			<p>9).</p> <p>The Keeper agrees that NRS have identified an appropriate individual to this role as required by the Act.</p>
<p>3. Policy</p>	<p>G</p>	<p>G</p>	<p>The Act requires an authority to have an appropriate policy statement on records management.</p> <p>NRS have a <i>Records Management Policy</i>. The Keeper has been provided with a copy of this <i>Policy</i>. This is version 7.0 dated May 2020.</p> <p>The <i>Records Management Policy</i> is publically available at https://www.nrscotland.gov.uk/record-keeping/records-policies/records-management-policy</p> <p>The <i>Records Management Policy</i> is specifically endorsed by Laura Mitchell, Director of Information and Records Services (see element 1) in a <i>Covering Letter</i> (see under General Comments below).</p> <p>The Keeper agrees that the <i>RMP</i> supports the objectives of the <i>Records Management Policy</i>.</p> <p>The <i>Records Management Policy</i> specifies that it does not apply to the archive collection held by NRS (section 2.2 - see also the Keeper's comments regarding the collection under element 4).</p> <p>The Keeper agrees that NRS has a formal records management policy statement as required by the Act.</p>

<p>4. Business Classification</p>	<p>G</p>	<p>G</p>	<p>The Keeper of the Records of Scotland (the Keeper) expects that the public records of an authority are known and are identified within a structure.</p> <p>NRS operate a hybrid system: Public records are held digitally on an electronic document and records management system (eDRM), on bespoke line-of-business systems and on shared drives (limited and principally legacy). There are also public records held in hard-copy format in-house. There are also hard-copy records held by a third party storage supplier.</p> <p><u>Digital eDRM:</u> NRS use the eDRM system of the Scottish Government (Objective) to manage their public records.</p> <p>The Keeper has been provided with an extract of the SG eDRM showing NRS records managed on that system.</p> <p>The Keeper has already agreed that the records management structure in the SG is appropriate (2015): https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/keepers-assessment-report-Scottish-government.pdf</p> <p><u>Digital Line of Business:</u> NRS operate several stand-alone systems with for example SAS (Statistical Analysis System) and GIS (Geo Spatial Information). These line-of-business systems sit outside eDRM, but the Keeper can agree that they are likely to allow the appropriate management of records within a structure as required.</p> <p><u>Digital Shared Drives:</u> The move to the use of the SG eDRM has occurred since the original agreement of the RMP by the Keeper (2013). This major piece of work is now complete. However, a small number of public records remain on the original Shared Drive system. This has been done for various reasons, principally because of format incompatibility.</p>
-----------------------------------	-----------------	-----------------	---

			<p>These Shared Drives have now been locked down and no new records are being managed on them. For the purposes of this assessment these can therefore be considered 'legacy' records. However, legacy records still require management and the Keeper acknowledges that he has been provided with details of the NRS 'network consolidation project' that is pursuing this. The Keeper has been provided with a copy of the <i>Legacy Shared Drives Review Guidance</i> document and a sample <i>Report</i> into this work. Once completed the 'network consolidation project' will be followed by a self-assessment using the Scottish Council on Archives ARMS tool (see under element 13 below)</p> <p><u>Physical in house:</u> Although the 'vast majority' of NRS's records are digital there are some hard-copy records. Hard-copy records are recorded in the eDRM and in the Information Asset Register (see below). The Keeper has been provided with details of the systems in place to ensure that NRS can be confident that these records can be stored, retrieved and destroyed/archived when appropriate.</p> <p><u>Physical external storage:</u> NRS employ the services of a long-term storage contractor for the management of some of its hard-copy records. The Keeper has been provided with details of the third party and of the systems set up with this supplier to ensure that NRS can be confident that the public records they hold are being robustly managed.</p> <p>NRS have also developed 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." (RMP page 9). A copy of the NRS IAR has been provided to the Keeper. He notes that it contains a good introductory explanation to help local business areas populate the Register. (See Local Records Management under General Comments below).</p>
--	--	--	--

			<p>The Keeper agrees that NRS retains all its public records in controlled systems which are structured in a clear manner and which can be used by staff to manage public records where appropriate.</p>
<p>5. Retention schedule</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects an authority to have allocated retention periods to its public records and for those records to be retained and disposed of in accordance with a Retention Schedule.</p> <p>NRS have provided the Keeper with the NRS <i>Retention Schedule</i>. This is version 5 dated May 2020. This features all record types in all formats.</p> <p>Destruction instructions are available to staff in the NRS <i>Records Disposal Policy</i> (see element 6).</p> <p>For the different formats featured in NRS records management systems see element 4 above. Specifically:</p> <p><u>Digital eDRM</u>: The vast majority of the public records of NRS are managed on the eDRM system of the Scottish Government where they currently make up part of the SG file plan. As such they are subject to the automated retention decisions of the SG. However, the Keeper is satisfied that NRS have adequate input to how these retention decisions are allocated to particular record types.</p> <p>The Keeper has already agreed that the retention processes of the SG, including e-mail retention, is appropriate (2015): https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/keepers-assessment-report-Scottish-government.pdf</p> <p><u>Digital Line of Business</u>: The Keeper can agree that records held on the various business systems (such as geo-spatial datasets) have specified retention decisions</p>

			<p>allocated and that these are understood.</p> <p><u>Digital Shared Drives:</u> Following a review of legacy public records that were not transferred to eDRM (for example for format compatibility reasons), NRS have ensured that retention rules have been imposed on these. Details have been provided to the Keeper in the <i>RMP</i> (page 11).</p> <p><u>Physical in-house:</u> Physical records are included in the NRS Retention Schedule (for example the audio tapes in the example above) and are tracked in eDRM. However, unlike digital records, paper records cannot be automatically deleted and must be manually destroyed. Staff guidance on how and when to do this has been provided as part of the NRS <i>Records Disposal Policy</i> (see element 6); for example at section 2.1</p> <p><u>Physical third party storage:</u> All public records held in the long term third party storage facility have retention decisions allocated. For the moment this is 'permanent preservation' for all records.</p> <p>There is a commitment in the RMP to keep the <i>Retention Schedule</i> subject to 'ongoing monitoring and annual review'. The Keeper notes that NRS actually review the <i>Schedule</i> biannually and this is commended. There are clear indications that NRS recognise a retention schedule as a living document that is likely to be subject to continual minor change year on year.</p> <p>The Keeper agrees that NRS has a schedule providing retention decisions for the record types created while pursuing its functions.</p>
6. Destruction Arrangements	G	G	The Act requires that public records are destroyed in a timely, controlled and secure manner.

			<p>NRS acknowledge this and set out that “Records management is about placing controls around...disposal whether this be recycling, confidential destruction or transfer to the archive branch (<i>Records Management Policy</i> – see element 3 – section 3.2). A commitment to pursuing this appears in the Policy at section 5.</p> <p>With this commitment in mind NRS has a <i>Records Disposal Policy</i> which has been provided to the Keeper. This is version 3.4 dated 17 May 2020. The <i>Records Disposal Policy</i> is available on the staff intranet.</p> <p>NRS have the following process in place, to ensure the controlled, secure and irretrievable destruction of public records (For the structure of NRS records management systems see element 4 above).</p> <p><u>Digital eDRM</u>: The vast majority of the public records of NRS are managed on the eDRM system of the Scottish Government where they currently make up part of the SG file plan. As such they are subject to the automated destruction processes of the SG.</p> <p>The Keeper has already agreed that the destruction processes in the SG are appropriate (2015): https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/keepers-assessment-report-Scottish-government.pdf</p> <p><u>Digital Line-of-Business</u>: These line-of-business systems sit outside eDRM, but the Keeper can agree that they are likely to allow the destruction of public records within a retention framework as required.</p> <p><u>Digital Shared Drives</u>: The Keeper acknowledges that he has been provided with details of the NRS ‘network consolidation project’ that is pursuing this. Part of this project is the deletion of records according to the NRS <i>Retention Schedule</i>. This was largely been done over the winter of 2017/18. NRS now intend to run a e-</p>
--	--	--	---

			<p>discovery programme on the legacy data to ensure all remaining records are accounted for and deleted when appropriate. The Keeper has been provided with a copy of the <i>Legacy Shared Drives Review Guidance</i> document and a sample <i>Report</i> into this work.</p> <p><u>Physical in-house</u>: The <i>Records Disposal Policy</i> describes procedures for the disposal of paper waste (confidential or otherwise). This work is undertaken by a third party contractor. NRS have provided the Keeper with destruction certificates as evidence that this arrangement is in operation.</p> <p><u>Physical third party storage</u>: All the public records held by the third party long-term storage provider are identified for permanent preservation. However, NRS have confirmed to the Keeper that they have considered the destruction issue with the supplier should the need ever arise.</p> <p><u>Hardware</u>: Hardware disposal is arranged through an automated system (iFix) and carried out by NRS Estates through a third party contractor. The Keeper has been provided with destruction certificates as evidence that this arrangement is in operation.</p> <p><u>Back-Ups</u>: The majority of the NRS public records are covered by the back-up processes of the SG. The Keeper has previously agreed that the destruction of SG back-up copies is controlled and understood. However, as explained in element 4 above some public records remain outside the eDRM. The RMP states (page 13) “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.”</p> <p>A copy of a <i>NRScotland Backup Procedure</i> document, confirming the above, has</p>
--	--	--	--

			<p>been provided to the Keeper.</p> <p>The Keeper agrees that NRS has processes in place to irretrievably destroy their records when appropriate.</p>
<p>7. Archiving and Transfer</p>	<p>G</p>	<p>G</p>	<p>The Act requires that all Scottish public authorities identify a suitable repository for the permanent preservation of any records considered suitable for archiving. A formal arrangement for transfer to that repository must be in place.</p> <p>NRS have identified their in-house archive as the proper repository for the small selection of their public records suitable for permanent preservation. The public records of NRS will therefore become part of the NRS collection (see explanation of the status of the collection under element 4 above).</p> <p>NRS is an accredited archive https://www.nrscotland.gov.uk/news/2015/national-records-of-scotland-receives-archive-accreditation-award and fully adheres to the Keeper's <i>Supplementary Guidance on Proper Arrangements for Archiving Public Records</i>: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/supplementary-guidance-on-proper-arrangements-for-archiving-public-records.pdf</p> <p>Although this is an in-house archive transfer, NRS have chosen to operate it under the terms of an internal memorandum of understanding (MOU). This has been supplied to the Keeper in evidence. The Keeper is satisfied that information asset owners (see under General Comments below) have adequate input to how preservation decisions are allocated to particular record types.</p> <p>The Keeper has also been provided with a copy of the NRS <i>Archiving Arrangements</i> document. This is version 1.3 dated 25 May 2020.</p>

			<p>The Keeper has also been provided with a copy of the NRS <i>Depositor Guidance for the Transfer of Archival Born Digital Records</i> which is available online https://www.nrscotland.gov.uk/record-keeping/guidance-for-depositors</p> <p>Staff guidance on preparing public records for archive transfer (particularly in the case of digital records) is available and has been shared with the Keeper.</p> <p>All NRS websites have been selected for preservation as part of the NRS Web Continuity Service: https://webarchive.nrscotland.gov.uk/</p> <p>As Deputy Keeper of the Records of Scotland, Laura Mitchell (see element 1) has management responsibility for the archive collection.</p> <p>The Keeper agrees that NRS has arrangements in place to properly archive records when appropriate.</p>
8. Information Security	G	G	<p>The Act requires that public records are held in accordance with information security compliance requirements.</p> <p>The RMP states (page 17): “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.”</p> <p>With this commitment in mind NRS have the following procedures in place to ensure the security of its public records:</p> <p><u>Digital eDRM</u>: The Scottish Government eDRM is governed by SG information security procedures. The Keeper has already agreed that these are appropriate</p>

			<p>(2015).</p> <p><u>Digital Line-of-Business</u>: The Keeper can agree that line-of-business systems operated by NRS have adequate information security provision as part of their functionality.</p> <p><u>Digital Shared Drives</u>: The Keeper has been provided with a copy of the <i>NRS Technical Security Standard</i> and agrees that in-house digital information security processes are appropriate.</p> <p><u>Physical in-house</u>: Access to paper records is restricted to appropriate staff with storage in locked rooms (a key sign-out system is in place) and a robust document tracking register is in place.</p> <p><u>Physical third party storage</u>: The third party storage provider utilises digital, physical and operational access controls at their facilities. They operate an Information Security Management System which complies with the requirements of ISO 27001.</p> <p>A system for reporting information security breaches (actual or potential) is in place. The Keeper has been provided with copies of the <i>NRS Incident Management Policy</i> and <i>Data Breach Reporting Guidance and Procedure</i>. Both are available to staff on the intranet.</p> <p>Vitality, all NRS employees are security cleared to the Baseline Personnel Security Standard, and undertake security awareness and data protection training.</p> <p>The Keeper notes that NRS have achieved Cyber Essentials + certification: Sector: Public administration and defence Certificate number: QGCE2190-14 Certificate level: Cyber Essentials Plus</p>
--	--	--	--

			<p>Date issued: 23/10/19</p> <p>The Keeper has intranet access to NRS information governance policies and guidance including the suite of information security guidance such as the <i>Access Control</i> or <i>Clear Desk</i> policies.</p> <p>The Keeper agrees that NRS have procedures in place to appropriately ensure the security of their records as required by the Act.</p>
9. Data Protection	G	G	<p>The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law.</p> <p>NRS is registered as a data controller with the Information Commissioner’s Office (ICO): https://ico.org.uk/ESDWebPages/Entry/Z2886501</p> <p>NRS have a <i>Data Protection Policy</i>. The Keeper has been provided with a copy of this <i>Policy</i>. This is version 1.1 dated May 2020. This is published at: https://www.nrscotland.gov.uk/record-keeping/legislation/primary-information-legislation/data-protection/data-protection-policy</p> <p>The <i>Data Protection Policy</i> confirms that “NRS is committed to ensuring that all of our employees comply with their obligations under the GDPR and the DPA 2018 and to safeguarding the integrity and confidentiality of any personal data held or processed by us.” (<i>Data Protection Policy</i> section 1.4)</p> <p>The <i>Data Protection Policy</i> explains the 6 principles of data protection (section 3).</p> <p>Service users can make a subject access request using an online template: https://www.nrscotland.gov.uk/files//record-keeping/legislation/nrs-data-protection-forms-subject-access-requests-application-form.pdf</p>

			<p>NRS have other relevant data protection information published on their website for example from: https://www.nrscotland.gov.uk/record-keeping/legislation/primary-information-legislation/data-protection</p> <p>NRS have committed to carrying out data protection impact assessments before they begin any processing of personal data which is likely to result in a high risk to individuals (<i>Data Protect Policy</i> section 6.2). With this in mind they have a <i>Data Protection Impact Assessment (DPIA) Policy and Guidance</i> document which has been provided to the Keeper. This is version 1.2 dated 26 May 2020.</p> <p>Furthermore, they have other supporting guidance for staff, such as an e-learning module. This has also been shared with the Keeper. The <i>Records Management Policy</i> (see element 3) specifically indicates support for the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), and the Data Protection Act 2018 (<i>Policy</i> section 2.4).</p> <p>NRS operates a Privacy Group to monitor data protection issues around projects; legislative and regulatory issues and to review information sharing requests. The Head of Information Governance (see element 2) is chair of the Privacy Group. The Keeper has been provided with this group's terms of reference.</p> <p>The Keeper has intranet access to NRS information governance policies and guidance including the suite of information security guidance such as the <i>Access Control</i> or <i>Clear Desk</i> policies.</p> <p>The Keeper notes that the Data Protection Policy covers records making up the collection at NRS. The inclusion of the collection under a single <i>Data Protection Policy</i> is laudable.</p>
--	--	--	--

			<p>The Keeper agrees that NRS have arrangements in place that allow them to properly comply with data protection legislation.</p>
<p>10. Business Continuity and Vital Records</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.</p> <p>NRS has an overarching <i>Business Continuity Plan (BCP)</i> that is advertised to staff on the intranet and located in eDRM. The Keeper has been provided with a copy. This is v1.0 dated September 2020.</p> <p>As well a central <i>BCP</i>, each area of NRS has operational business continuity plans. These have been provided to the Keeper and he agrees that they include provision for record recovery in an emergency.</p> <p>The Head of Information Governance (see element 2) authorised the sample <i>Business Continuity Plans</i> received by the Keeper.</p> <p>Vital records are identified in the NRS Retention Schedule (see element 5 above)</p> <p>The majority of the NRS public records are held on the SG eDRM system which has full continuity back-up. The Keeper has already agreed that the records recovery provision in the SG is appropriate (2015): https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/keepers-assessment-report-Scottish-government.pdf</p> <p>NRS have also developed a disaster recovery plan for the public records that did not transfer to eDRM.</p> <p>NRS have provided the Keeper with technical details of the processes in place at</p>

			<p>the third-party storage contractor and he agrees they have properly considered disaster planning.</p> <p>NRS has commitment to “The review and ongoing development of NRS business continuity planning, encompassing strategies to ensure that vital records held by NRS remain accessible over time and that there are processes in place to monitor the integrity, security and usability of records.” (<i>Records Management Policy</i> Section 5.1).</p> <p>The Keeper has intranet access to NRS information governance policies and guidance including those relevant to business continuity.</p> <p>The Keeper agrees that NRS have an approved and operational business continuity process and that information management and records recovery properly feature in the authority’s plans.</p>
11. Audit trail	G	G	<p>The Keeper expects an authority to have process in place to track public records in such a way that their location is known and changes recorded.</p> <p>The <i>Records Management Policy</i> (see element 3) states that “Records management is about placing controls around each stage of a record’s lifecycle, at the point of creation (through the application of metadata, version control and naming conventions...(through the management of security and access classifications, facilities for access and tracking of records)...By placing such controls around the lifecycle of a record, we can ensure they demonstrate the key attributes of authenticity, reliability, integrity and accessibility...this may be achieved through the management of effective metadata as well as the maintenance of comprehensive audit trail data. (<i>Policy</i> sections 3.2 and 3.3). It is clear NRS recognise the importance of locating, tracking and correctly identifying records.</p>

			<p>With this in mind, NRS have the following processes in place (For the structure of NRS records management systems see element 4 above.)</p> <p><u>Digital eDRM:</u> The vast majority of the public records of NRS are managed on the eDRM of the Scottish Government (Objective) where they currently make up part of the SG file plan. The Objective system has a powerful search facility that allows a user to track all records using a variety of search criteria. The efficiency of the search facility relies on consistent naming of documents as they are saved as records on the system.</p> <p>NRS have a <i>Document Naming and Control Guidelines</i> document which has been provided to the Keeper. This is version 3.1 approved by the Director of Information and Records Services (see element 1) on 15th May 2020. The author of the <i>Guidelines</i> is the Head of Information Governance (see element 2). The Keeper agrees that this gives clear and appropriate instructions to staff to ensure that records are named on the eDRM in such a way as will allow tracking. The eDRM itself automatically imposes version control.</p> <p><u>Digital Line-of-Business:</u> NRS operate line-of-business systems such as SAS (Statistical Analysis System). The Keeper can accept these systems have record tracking functionality.</p> <p><u>Digital Shared Drives:</u> Public records still held on corporate shared drives have been largely located and identified. NRS intend to double check using an e-discovery tool shortly. Once legacy public records have been identified they are 'locked' in place. NRS state in the <i>RMP</i>: "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." (<i>RMP</i></p>
--	--	--	---

			<p>page 24)</p> <p><u>Physical in-house</u>: Legacy paper files have been added to the eDRM and IAR listing and can only be accessed through a controlled system which provides an electronic register of file movement. At any given time the location of a paper record should be immediately identified. The Keeper has been provided with a sample from the Paper Records Management System Audit Trail as evidence that this arrangement is operational.</p> <p><u>Physical third party storage</u>: NRS uses an online document tracking system provided by the third party contractor as part of their contract. The Keeper is satisfied that, at any time, the NRS would be able to identify and retrieve the records held in that long-term storage facility.</p> <p>The Keeper agrees NRS has procedures in place that will allow them to locate their records and assure themselves that the located record is the correct version.</p>
<p>12. Competency Framework for records management staff</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.</p> <p>NRS has commitment to “The identification of records management as a distinct stream within the organisation’s training portfolio, with dedicated training provided to all staff.” (<i>Records Management Policy</i> Section 5.1).</p> <p>NRS state: “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...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.” (RMP page 26) (see Local Records Management under General Comments below).</p>

			<p>Staff undergo mandatory data protection training annually and NRS is developing a similar information security training module at the moment. The Keeper requests that he is informed when this is approved and rolled out. The Keeper acknowledges he has been provided with sight of the Data Protection e-learning module.</p> <p>Updates to information governance policies and guidance will be disseminated to all colleagues via the corporate intranet and e-mail network (<i>Records Management Policy</i> section 9.1)</p> <p>The Keeper has been provided with a copy of the NRS <i>Induction Welcome Pack</i>. He agrees that information governance is suitably represented and, in particular, that there is a section dedicated to robust records management (<i>Welcome Pack</i> section 9). New staff have to acknowledge that they have received and understood the <i>Welcome Pack</i>.</p> <p>Staff training in records management is fully supported by section 8 of the NRS <i>Records Management Policy</i>.</p> <p>The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, he agrees that NRS consider information governance training for staff as required.</p>
<p>13. Assessment and Review</p>	<p>G</p>	<p>G</p>	<p>Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.</p> <p>The RMP is reviewed annually with a first review scheduled for May 2021 (<i>RMP control sheet</i>).</p>

			<p>Reviewing the implementation of the <i>RMP</i> is the responsibility of the Head of Information Governance (see element 2) supported by the NRS Information Governance Team (see under general comments below).</p> <p>To inform the 2021 review NRS intend to self-evaluate using the Scottish Council on Archives' ARMS framework. This follows an earlier Data Management Maturity assessment (February 2020). The Keeper would be interested in the results from the ARMS exercise. The Keeper acknowledges that he has been provided with a copy of the Data Management Maturity assessment.</p> <p>The results of any review are reported to the Executive Management Board. The Director of Information and Records Services (see element 1) sits on this Board. The Executive Management Board is responsible for monitoring the Information Strategy and Work Plan (<i>NRS Governance Boards Terms of Reference</i>).</p> <p>As well as the assurance of an overall <i>RMP</i> review, most individual elements have an annual review commitment and details of who should carry out that review. For example: "The competency framework and training requirements will be reviewed annually by the Information Governance and People Services teams." (<i>RMP</i> page 27)</p> <p>The <i>Data Protection Impact Assessment (DPIA) Policy and Guidance</i> (see element 9) must be reviewed by November 2020.</p> <p>The NRS <i>Retention Schedule</i> (see element 5) must be reviewed by December 2020.</p> <p>The Records Management Policy (see element 3), the <i>Data Protection Policy</i> and the Personal Data Breach Reporting: Procedure and Guidance (see element 9), the NRS Business Continuity Plan (see element 10), the <i>Document Naming and Control</i></p>
--	--	--	---

			<p><i>Guidelines</i> (see element 11), the <i>Data Sharing Guidelines</i> (see element 14) and the <i>Records Disposal Policy</i> (see element 6) must all be reviewed by May 2021.</p> <p>The Records Management Competency Framework must be reviewed by April 2022.</p> <p>The Archiving Arrangements document (see element 7) must be reviewed by May 2022.</p> <p>The Clear Desk Guidance document (see element 8) must be reviewed by July 2022.</p> <p>The Keeper agrees that NRS have made a firm commitment to review their <i>RMP</i> as required by the Act and have explained who will carry out this review and by what methodology. Furthermore he agrees that supporting policy and guidance documents have appropriate review periods allocated.</p>
14. Shared Information	G	G	<p>The Keeper expects a Scottish public authority to ensure that information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.</p> <p>NRS state in their <i>Records Management Policy</i> (section 4.2) that one of the benefits of implementing records management systems and processes is improved information sharing and the provision of quick and easy access to the right information at the right time (see also element 11).</p> <p>NRS shares information with third parties and does so “using transparent and proportionate controls and robust security processes” (<i>RMP</i> page 30) including the use of Data Sharing Agreements and a central register of agreements. The Keeper has been provided with the <i>Data Sharing Template</i>, a sample from the <i>Register</i> and</p>

			<p>a <i>Data Sharing Agreement</i> (with the University of Edinburgh) all as evidence that the arrangements explained in the <i>RMP</i> are currently operational.</p> <p>NRS staff are provided with guidance around information sharing on the corporate intranet. The Keeper has been provided with a copy of the <i>NRS Data Sharing Guidelines</i>. This is version 1.2 dated 15 May 2020.</p> <p>NRS uses eDRM Connect, the Scottish Government endorsed collaboration tool for added control of public records when they are shared or jointly created.</p> <p>To further their commitment to transparency and open data NRS explain that “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” (<i>RMP</i> page 30).</p> <p>The Keeper notes that NRS is “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”. (<i>RMP</i> page 31). The Keeper requests he is updated as this project progresses.</p> <p>The Keeper can agree that NRS properly considers records governance when undertaking information sharing programmes.</p>
<p>15. Public records created or held by third parties</p>	<p>N/A</p>	<p>N/A</p>	<p>The Keeper expects a public authority to ensure that adequate arrangements are in place for the management of records created and held by third parties who carry out any functions of the authority.</p> <p>This is acknowledged in the <i>RMP</i> (page 4).</p> <p>However, NRS are clear that they have “not tasked any third parties to carry out its</p>

			functions.” The Keeper agrees that this element does not apply to these authorities.
--	--	--	---

**Keeper of the Records of Scotland and Registrar General of Births Deaths and Marriages for Scotland
(for simplicity the separate authorities will be referred to as ‘NRS’ in the assessment below)**

Version: This assessment is on the Keeper of the Records of Scotland and Registrar General of Births, Deaths and Marriages for Scotland (NRS) Records Management Plan (the *RMP*). This is version 3.0 of the *RMP* approved on 28 September 2020. The *RMP* was prepared by the Head of Information Governance (see element 2) and approved by the Director of Information and Records Services (see element 1). The Keeper originally agreed the *Records Management Plan* of NRS in 2013: <https://www.nrscotland.gov.uk/files/record-keeping/public-records-act/20130704Keeper%27sAssessmentReport.pdf> the authority submitted a Progress Update Review (PUR) in 2017: <https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/pur-final-report-for-national-records-of-scotland.pdf>

The authority refers to records as a business asset (for example *RMP* page 9 or *Records Management Policy* - see element 3 - page 3). This is an important recognition and the Keeper commends it.

The Keeper agrees that the efficiencies introduced by robust records management provision will assist NRS to attain the objectives explained in the *Corporate Plan*:
<https://www.nrscotland.gov.uk/about-us/corporate-planning>

The *RMP* mentions the Act and is based on the Keeper’s, 15 element, Model Plan <http://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan>.

The *RMP* is already available on the NRS website at: <https://www.nrscotland.gov.uk/files//about-us/nrs-records-management-plan-may-2019.pdf>

Key Group: NRS Information Governance Team (IGT)

NRS have established an IGT which is responsible for supporting the implementation of the RMP. They offer advice and support to NRS staff in all matters relating to information.

The IGT provide support and deliver training where appropriate.

The IGT are responsible for monitoring and reviewing aspects of the RMP, such as access control or training requirements, and for liaising with other groups in NRS when this is relevant. For example under element 6 (Destruction) the IGT works with the IT Security Team in its annual review of arrangements.

Local representatives (see below) are responsible for highlighting any records management issues or concerns to the IGT.

The IGT is specifically charged with supporting the Data Protection Officer (see element 1) (*Data Protection Policy* section 7.3). They sign-off high risk processing following a DPIA.

Local Records Management:

There is ample evidence in the *RMP* that NRS have designed their records management provision with close engagement with local business areas in mind. For example: “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.” (*RMP* page 28). This is to be commended.

In particular records management responsibility has been shared with local ‘champions’ in each business area. These fall in to two categories records ‘Information Asset Owners’ and ‘Support Officers’ (IMSOs).

Information Asset Owners are responsible for “ensuring proper management and secure disposal of their information assets.”

Information Asset Owners are responsible for liaising with the Head of Information Governance (see element 2) around Freedom of Information Requests and the appraisal their records with permanent retention (see element 7) in mind.

Information Asset Owners are responsible for allocating access rights to records and to periodically review those rights (*Access Control Policy* section 3.1) and to ensure their staff are familiar with their local procedures for reporting incidents (*Incident Management Policy* section 4.3)

Information Asset Owners are responsible for accepting the privacy risks and solutions identified in a Data Protection Impact Assessment (see element 9) and for deciding whether to publish any DPIAs relating to the records allocated to them. A DPIA must be signed off by an Information Asset Owner (*Data Protection Impact Assessment Policy and Guidance*).

Support Officers (described in the RMP as 'gatekeepers of eDRM') within directorates are responsible for offering advice and guidance regarding records management to all staff within their branch (*Records Management Policy* section 6.4). They monitor the compliance with relevant policies and guidance in consultation with the Head of Information Governance (see element 2)

They have day to day responsibility for ensuring the eDRM is being operated correctly in their business area and for correcting naming errors. They are also the point of contact in a business area for file creation in eDRM (although files are created centrally by the SG).

Both levels of local representative are responsible for highlighting any records management issues or concerns (including around security) to the IGT (see above).

Clearly these local 'champions' are vital to the records management process in NRS and the Keeper thanks the authority for sharing details of their remit as part of this submission.

6. Keeper's Summary

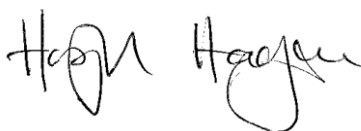
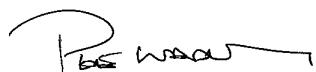
Elements 1 - 15 that the Keeper considers should be in a public authority records management plan have been properly considered by the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland. Policies and governance structures are in place to implement the actions required by the plan.

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper agrees the RMP of the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland.

- The Keeper recommends that these authorities should publish their agreed RMP as an example of good practice within the authority and the sector.

This report follows the Keeper's assessment carried out by,



.....
Pete Wadley
Public Records Officer

.....
Hugh Hagan
Senior Public Records Officer

8. Endorsement of Report by the Keeper of the Records of Scotland

The report has been examined and is endorsed under the signature of the Keeper of the Records of Scotland as proof of compliance under section 1 of the Public Records (Scotland) Act 2011, and confirms formal agreement by the Keeper of the RMP as submitted by the Keeper of the Records of Scotland and the Registrar General of Births Deaths and Marriages for Scotland. In agreeing this RMP, the Keeper expects these authorities to fully implement the agreed RMP and meet their obligations under the Act.



.....
Paul Lowe
Keeper of the Records of Scotland