National Records of Scotland

Public Records (Scotland) Act 2011

**Keeper of the Registers of Scotland
Assessment Report**

The Keeper of the Records of Scotland

17 January 2017

Contents

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 Registers of Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 31 May 2016.

The assessment considered whether the RMP of the Keeper of the Registers of 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 Registers of Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

Registers of Scotland (RoS), which carries out the functions of the Keeper of the Registers of Scotland, is the non-ministerial government department responsible for compiling and maintaining 17 public registers. These relate to land, property, and other legal documents. The main registers are the Land Register of Scotland and General Register of Sasines.

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 Registers of Scotland 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

Element	Present	Evidence	Notes
1. Senior Officer *Compulsory element*	G	G	The Records Management Plan (RMP) identifies Janet Edgell, Operations Director, as the senior manager with strategic responsibility for records management within RoS. Ms Edgell has included an introductory section to the RMP highlighting her commitment to achieving best practice recordkeeping standards. The RMP also includes an introduction from Sheenagh Adams, Keeper of the Registers of Scotland, which underlines her support for the development of the RMP. Ms Edgell is also RoS's Senior Information Risk Officer (SIRO) and Accountable

			Officer. She is also a Member of the Board of Directors and Chairs the Information Assurance Group and the Executive Management Team. Ms Edgell also reports directly to the Keeper of the Registers of Scotland. A description of the Governance Framework has been supplied as evidence (Annex D). Ms Edgell's role profile has been submitted as evidence (Annex E) and shows a responsibility for information governance. Ms Edgell's role is also confirmed in the Records Management Policy (Annex G). A link to Ms Edgell's profile as member of the Board has also been supplied. This is available on RoS's website. The Keeper of the Records of Scotland (the Keeper) agrees that an appropriate individual has been identified to take senior management responsibility for records management as required by the Public Records (Scotland) Act 2011 (PRSA).
2. Records Manager *Compulsory element*	**G**	**G**	The RMP identifies Alison Kendall, Records Manager, as having operational responsibility for records management within RoS. The RMP states that Ms Kendall is responsible for implementing the RMP and the improvement plan. Ms Kendall is also a member of the Information Governance Team. Representatives from the Team attend meetings of the Information Assurance Group which reports regularly to the Executive Management Team and the SIRO (see Element 1) on information risk and compliance issues. Ms Kendall's Role Profile is submitted as evidence (Annex E). This clearly shows that she has responsibility for records management within RoS. She reports to the Data Protection Officer. **The Records Management Policy (Annex G) identifies Aidan Robertson as**

	G	**G**	**RoS's Records Manager. The Keeper accepts that Mr Robertson was responsible for records management prior to the appointment of Ms Kendall and recommends that the text of the Policy is amended when it is next reviewed to reflect that Ms Kendall is now the Records Manager.** The Keeper agrees that an appropriate individual has been identified to take day-to-day responsibility for records management as required by the PRSA.
3. Policy *Compulsory element*	**G**	**G**	RoS has submitted its Records Management Policy (Annex G) which was last updated and approved by the Policy and Practice Group in March 2016 (version 1.0) and is next due for review in March 2018. It sets out RoS's corporate approach to records management and specifically states that although the Registers created and maintained by RoS are not managed as public records as part of the provisions set out in the RMP, they will be managed to best practice standards similar to the corporate records created and managed by RoS in support of the creation of the Registers. The Policy sets out the roles and responsibilities of staff, including the confirmation of the individuals identified in Elements 1 and 2, and shows a commitment to staff training and providing relevant guidance in relation to aspects of records management. Appendix B of the Policy provides staff with a useful tool for differentiating between documents and records. Screenshots of the Information Governance and PRSA areas of RoS's intranet have been supplied (Annex F) showing the location of the Policy thus ensuring that staff have access to it and are therefore aware of their responsibilities. The slides of the Information Governance presentation given at RoS's corporate induction have also been provided (Annex H). These show that staff receive initial training in information governance and records management when they join the organisation. The Keeper commends this commitment to providing staff with

			appropriate training.
			The Policy forms a key part of RoS's Information Governance Strategy and Improvement Plan 2016-2018 (Annex B). This provides an overview of the high level aims over the coming years and outlines 9 key objectives to achieve, including clearly articulating and communicating key policy commitments and ensuring that staff are aware of their roles and responsibilities.
			The RMP explicitly states that none of the Keeper of the Registers' functions, either statutory or corporate, are carried out by a third party.
			The Keeper agrees that RoS has outlined its policy towards records management and has shown a commitment to training staff to be able to comply with the Policy.
4. Business Classification	**A**	**G**	The RMP states that a considerable amount of work has been undertaken with business areas to develop a Business Classification Scheme (BCS), which has been submitted as evidence. The Keeper commends the liaison with local service areas to develop the BCS as this will lead to a stronger business tool. The BCS follows a three level functional framework showing the functions, activities and transactions. Although this must remain a business decision for any authority, the Keeper recognises that the functional approach is currently recognised as best practice as it is likely to be more resilient in the event of any business re-organisation.

The RMP also states that the BCS is maintained by the use of a 'Wiki' application. The Wiki is essentially similar to an intranet page in that it is available to all staff, but it also contains functionality which allows the Information Governance Team to edit the page and keep it up-to-date. Staff are able to see the top level description of the categories of records but can then use links to identify the more detailed lower levels. The BCS is reviewed regularly and changes are triggered by updates made to the Information Asset Register, samples of which have been submitted alongside |

<table>
<tr><td></td><td colspan="2"></td><td>the BCS.

Also submitted as evidence is an Information Appraisal Template (Annex I) which is used to identify information and record types.

The Records Management Improvement Plan 2016-2019 (Annex C) highlights the need to carry out remedial work on shared drive and Outlook areas of the network and for full roll-out and implementation of the BCS. The work to re-design and imposition of the corporate fileplan on areas of the shared drives will be used to also dispose of records and information that is no longer required. The Keeper requests that he is kept informed of the work to roll-out the BCS structure across the authority.

The Keeper can agree this Element on an 'improvement model' basis. This means that the authority has identified a gap in provision (a fully operational BCS) and has identified how it intends to close this gap. This agreement is dependent upon the Keeper being kept informed of progress of work in this area.</td></tr>
<tr><td>5. Retention schedule</td><td>**G**</td><td>**G**</td><td>Alongside the work in developing its BCS, RoS has produced a consolidated Retention and Disposal Schedule (RDS) which is in the form of a spreadsheet and has been submitted as evidence. It follows the same three tiered structure of the BCS and outlines the retention and disposal actions to be taken against the classes of records created and the time periods after which these occur. It also notes vital records, level of security classification and the individual responsible for authorising disposal. HR has its own more detailed section within the RDS. The Registers maintained by RoS also appear on the RDS.

The RMP states that the RDS is available to staff on the corporate intranet. Annex F shows the location of the RDS on RoS's intranet site.</td></tr>
</table>

			Guidance on using the RDS has also been provided on the intranet site. A screenshot of this has been provided as evidence (Annex J). Also submitted is a staff notice from RoS's intranet (Annex K) which shows the consultative manner in which the RDS was developed. The Keeper commends this approach as one which is likely to engender greater 'buy-in' from staff and is therefore more likely to be an effective business tool. The Keeper agrees that RoS has an operational retention schedule and disposal schedule which outlines the actions to be taken against classes of records at the end of their lifecycle.
6. Destruction Arrangements *Compulsory element*	**A**	**G**	The RMP outlines the following destruction arrangements: **On-site paper records** – Where records contain sensitive or personal information they are shredded by staff on-site. Records which are not confidential are placed into secure consoles which are placed around RoS's buildings. These are then collected daily and are destroyed securely off-site by a third-party contractor, Carillion. The contractor is obliged to comply with ISO 27001 and other secure waste disposal standards. Upon secure destruction of physical records a destruction certificate is generated and issued to RoS, where it is then managed as a corporate record and is subject to the requirements of the RDS. Sample destruction certificates have been supplied as evidence (Annex N). **Off-site paper records** - Records stored off-site by a third-party contractor (Iron Mountain) are destroyed securely under instruction from RoS. The Framework Agreement (Annex O) states that the provider must provide auditable process for the destruction of information. The contractor's Destruction Process flowchart has also been supplied. The RMP states that destruction certificates are provided to RoS which are then retained as corporate records. A sample destruction certificate for the secure destruction of paper records stored off-site has been supplied as

evidence.

Electronic records – The RMP states that a limited number of records are managed by an Electronic Document and Records Management System (EDRMS) called Vignette VRD. Auditable metadata stubs are maintained when records are destroyed. A screenshot (Annex AI) has been supplied showing the destruction record maintained when records are deleted from the system.

The RMP contains a description of the procedures for ensuring records managed on shared drives are routinely disposed of when required. Awareness of the Retention and Disposal Schedules has been raised across the organisation. Notification of destruction is identified on a quarterly basis by Area Information Managers and destruction of these takes place locally with the assistance of the Records Manager. The recording of the disposal of records forms part of the RM Improvement Plan 2016-2019 (Annex C). A sample destruction form has been submitted as evidence (Annex AN).

Hardware – The RMP indicates that hardware, storage devices and mobile devices are destroyed on-site by an approved contractor. The evidence submitted (Annex M) shows the key points of the contractual arrangements and also includes a destruction log and a sample destruction certificate. These are maintained as corporate records and are subject to the requirements of the RDS.

Back-ups – The RMP states that electronic records are subject to at least a daily back-up regime. Records deleted from RoS systems will remain on back-ups until overwritten. The RMP states that back-ups are retained for six months before being overwritten.

RoS has supplied Destruction and Transfer Guidelines (Annex L) which provides staff with advice on how to dispose of paper records hold on- and off-site and also

			on how to transfer records on a regular basis to the National Records of Scotland (NRS). Annex A to this document provides a template form which should accompany records transmissions to NRS. **The Keeper can agree this Element on an 'Improvement Model' basis. This means that the authority has identified a gap in provision (the recording of the destruction of electronic records managed on shared drives) and has evidenced a commitment to closing this gap. As part of this agreement the Keeper requests that he is kept informed of the progress of the work to close this gap.**
7. Archiving and Transfer *Compulsory element*	G	G	The RMP has identified NRS as its designated archive. RoS and NRS have a long standing transfer arrangement for both RoS's corporate records and the statutory registers. A Memorandum of Understanding (MoU) has been developed to govern the arrangements for the transfer of records selected for permanent preservation. RoS has submitted a signed copy of the agreed MoU. The Destruction and Transfer Guidelines document (Annex L) outlines the practical procedures for transferring records to NRS. RoS has also submitted its Information Continuity Strategy (Annex P). This outlines the organisation's commitment to ensuring that the information that it creates and maintains continues to be accessible. The records created by RoS are of fundamental importance to Scottish land and property ownership. The Strategy shows a commitment to making sure that RoS can maintain the integrity, security and accessibility of the records it creates in perpetuity, in both paper and electronic format. The Keeper agrees that appropriate arrangements are in place to transfer records selected for permanent preservation to a suitable archive.

| 8. Information Security *Compulsory element* | G | G | RoS has submitted its Information Security Policy (Annex Q) which was approved by the Information Assurance Group, which is chaired by the SIRO (see Element 1) in March 2015. The Policy describes RoS's commitment to ensuring the security of the records it creates and manages, irrespective of format or the media on which it is stored. The SIRO has overall responsibility for information security, but in practice this is delegated to a Departmental Security Officer (DSO) and a series of Information Asset Owners (IAOs).

The Information Assurance Group is responsible for managing the information risk management framework.

The Policy is supported by a suite of policies and guidance. These include: an Information Assurance Handbook (Annex R) which covers identifying and managing information assets, information risks and data sharing; an Access Control Policy (Annex S) which governs staff access to RoS information and systems; an Email Policy (Annex T); a Security Classification Policy (Annex U) which determines the levels of security to be applied to information and records; and a Password Policy (Annex V). All these and other policies and guidance are available on the Security and Information Assurance area of RoS's intranet and a screenshot evidencing this has been submitted (Annex Y).

Also submitted is an extract from the Security Improvement Plan which shows that RoS is committed to continually improve its security provisions.

The Role Profile for the Security Manager has been provided (Annex E).

RoS's IT Information Security Management System is also certified as being compliant with ISO 27001:2013 and the certificate has been supplied as evidence (Annex W). |

			The RMP states that all staff are required to undertake training on the Responsible for Information eLearning module every two years. At induction, new members of staff are introduced to information security staff and relevant information policies and procedures. A sample of the information governance slides presented to staff at induction have been submitted (Annex H). The RMP states that paper records, maintained mainly by Finance and Human Resources, containing personal or sensitive information are secured in locked cabinets or rooms and cupboards where access is controlled by a passcode. Only those staff who require access to these records are provided with the passcodes. Submitted as evidence is RoS's Clear Desk and Screen Policy (Annex AM). Also submitted is guidance for staff in Human Resources/Finance/Legal Services in handling and disposing of sensitive information (Annex AL). The Keeper agrees that there are robust procedures in place to ensure that information and records are afforded the appropriate protection and that staff are made aware of their responsibilities.
9. Data Protection	G	G	RoS has submitted their Data Protection, Privacy and Confidentiality Policy (Annex Z) which demonstrates the organisational commitment to complying with the Data Protection Act 1998 and other information legislation with a view to embedding compliance as 'business as usual'. The Policy allocates senior responsibility for Data Protection to the SIRO (see Element 1) with operational responsibility assigned to the Data Protection Officer (see Element 2). The Policy also shows a commitment to ensuring that all staff are provided with training to ensure they are aware of their responsibilities. The Keeper commends this commitment. The Policy was approved by the Policy Group in March 2016 and is due for review in March 2018. The Policy is available to staff on RoS's intranet site and a screenshot has been supplied evidencing this (Annex F). RoS employs a professionally qualified Data Protection Officer (see Element 2) who

			regularly reports to the SIRO and the Head of Legal Services. The Keeper of the Registers of Scotland is registered as a Data Controller with the Information Commissioner's Office (registration number: Z5397958). RoS's website includes a Privacy Statement which details how it manages personal data and cookies and an Information Charter which provides information about how to request access to personal data. The Keeper commends this external provision of information for RoS's stakeholders. The RMP states that RoS undertakes Privacy Impact Assessments whenever it changes how it processes personal data or undertakes new processing. A template assessment form has been supplied as well as a sample completed form for a project to replace BlackBerry devices (Annexes AA and AB). When data processing is undertaken by a third party appropriate clauses are inserted into Data Processing Agreements. A sample Agreement between RoS and Revenue Scotland has been provided as evidence (Annex AC). The Keeper agrees that RoS is aware of its responsibilities under the Data Protection Act 1998 and has robust procedures in place to protect the personal data it creates, collects and manages.
10. Business Continuity and Vital Records	G	G	The RMP describes the Business Continuity Management (BCM) arrangements it has in place. It operates a high-level strategic BCM Plan, an extract of which has been provided as evidence (Annex AD) showing the proposed responses to a number of potential scenarios. The Strategic Plan is supported by a number of local area and critical business plans. A sample extract from the Plan for eServices has been provided showing the provision at a local level (Annex AE). The abovementioned plans are regularly reviewed and tested and are subject to

			external audit. An Outcome Report for a business continuity exercise which took place in March 2013 has been supplied (Annex AF) showing that testing of the provisions takes place. RoS maintains its BCM plans and procedures on a third party provided cloud platform ensuring it is available in the event of a disaster. Vital records are identified in the RDS, which is agreed between Information Asset Owners and business continuity managers. Where relevant vital records are included in operational BCM plans. The RMP states that data is backed up nightly and replicated across multiple site servers which has automatic back-up and recovery procedures in place. RoS's IT division is accredited to ISO 22301 standard for its Business Continuity Management System (Annex W). The Keeper agrees that robust procedures are in place to ensure that information and systems are restored in the event of an interruption to normal business patterns.
11. Audit trail	A	G	The RMP states that RoS currently manages a large amount of paper records although this is likely to reduce substantially as it aims to conduct more of its registration activities electronically as part of its Business Transformation Programme. At present, registration documentation received by RoS is scanned on arrival and managed as a digital record. In terms of paper corporate records, the vast majority are HR and Finance files. While these are still current/semi-current the RMP states that these are managed in-office. In these business areas, records are stored in secure lockable cupboards with access limited to only those staff with a business requirement to use them. Staff are not permitted to remove records from the office environment. The RMP states

that access to individual files is not tracked but there is a commitment to improve in this area and this is highlighted in the IM Improvement Plan 2016-2019 (Annex C). The RMP also states that once records are no longer regularly required for business purposes they are subject to an inventory of storage, movement and access both on-site and with the off-site storage provider. A sample of the off-site inventory has been provided as evidence.

RoS currently manages its digital records across a range of platforms. The Vignette EDRMS is used to manage a limited amount of electronic records. A sample of the audit trail functionality has been submitted as evidence (Annex AI) which shows the history of actions taken against the records stored on the system. RoS is currently looking at migrating these records to an alternative system as the Vignette system is approaching the end of its useful life. The Keeper requests that he is kept informed of developments in this area.

The RMP states that the Registration Manual, which is a core information resource and corporate record, is maintained using a wiki application. The Manual is continually updated and changes are recorded. A sample of the metadata captured when alterations are made has been supplied as evidence (Annex AI).

Many electronic corporate records are managed on a shared drive structure which lacks the functionality to be able to track changes made to and movements of records. The RMP states that there are areas of good practice, for example, Legal Services which operates a document naming convention (Annex AH). The RMP recognises the need to extend provision to all areas and this is built into the Records Management Improvement Plan 2016-2019 (Annex C). The Keeper requests that he is kept informed of work in this area.

Also submitted as evidence is a document which details the Baseline Technical Requirements for Record-keeping Systems (Annex J) which specifies the

			requirements for a system to be able to provide in the future to meet the needs of RoS. It includes metadata requirements and the need to monitor access and the history of actions taken against the record. **The Keeper can agree this Element on an 'improvement model' basis. This means that the authority has identified a gap in provision (the lack of an organisation-wide ability to track changes to and movement of records) and has evidenced a commitment to closing this gap. As part of this agreement the Keeper will expect to be kept informed as work in this area progresses.**
12. Competency Framework for records management staff	**G**	**G**	Both the Data Protection Officer (see Element 2) and the Records Manager are professionally qualified records management practitioners. Their Role Profiles have been provided as evidence (Annex E) which clearly show a responsibility for information governance and records management. RoS has recently undertaken work to develop a competency framework relating to information governance for all of its staff. It has been based on the Government Information and Knowledge Management framework but has been tailored to fit RoS's needs. Submitted as evidence is the Information Governance Competency and Training Matrix which details the necessary skills required for the information specialists within RoS but also for all staff. The RMP states that there is a commitment to apply the competencies to the roles of relevant staff and to provide them with the training to carry these out. This is also built in to the Records Management Improvement Plan. Training provision for staff has been evidenced elsewhere in the RMP. All new members of staff are required to undertake training in information governance. In addition, on a two-yearly basis all staff are required to complete an eLearning module, Responsible for Information, which includes information handling and security aspects.

	G	G	The Keeper agrees that the individuals responsible for the implementation and maintenance of records management systems within RoS have the necessary skills and access to training to be able to carry out their roles.
13. Assessment and Review	G	G	The RMP states that the RMP is owned by the Information Assurance Group, which is chaired by the SIRO (see Element 1), who will be responsible for reviewing it at least annually. This is confirmed in an extract from the minutes of a meeting of the Group in May 2016 (Annex AG). Improvement actions relating to the RMP will be reviewed on a quarterly basis. The Information Assurance Group reports to the Executive Management Team, who approved the improvement plan at a meeting in January 2016 (Annex AG). The Information Assurance Group owns the improvement plan and will be responsible for taking these actions forward. The Records Management Improvement Plan (Annex C) sets out how RoS intends to review its records management systems on an annual basis. Targets and outcomes will be defined and the review will take place to measure whether these have been achieved. This will be monitored by an online survey. A sample of the records management review survey has been supplied as evidence (Annex AK). The Keeper can agree that there are measures in place to ensure that RoS's RMP and supporting policies and procedures are reviewed and updated regularly.
14. Shared Information	G	G	The RMP states that RoS routinely shares information with a number of stakeholders. When a decision is made to participate in the sharing of information, the arrangements will be governed by a data sharing agreement. An extract from a sample Data Sharing Agreement between RoS and Revenue Scotland has been submitted as evidence. This shows that there are appropriate Information Governance and security controls in place to allow information to be shared securely and that each partner's responsibilities are clearly defined.

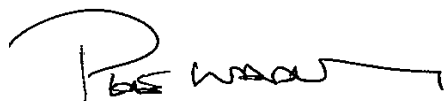|			
			Where it is deemed necessary, prior to entering into an Agreement a Privacy Impact Assessment and /or an Information Management Technical Risk Assessment (IMTRA) will be carried out. The Keeper agrees that there are appropriate procedures in place to allow the secure sharing of information and that information governance is considered when sharing information with other organisations.

6. Keeper's Summary

Elements 1-14 that the Keeper considers should be in a public authority records management plan have been properly considered by the Keeper of the Registers of 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 Registers of Scotland.

The Keeper recommends that the Keeper of the Registers of Scotland should publish its 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   **Robert Fotheringham**
Public Records Officer   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 Registers of Scotland. In agreeing this RMP, the Keeper expects the Keeper of the Registers of Scotland to fully implement the agreed RMP and meet its obligations under the Act.

……………………………………………

Tim Ellis
Keeper of the Records of Scotland