National Records of Scotland

Public Records (Scotland) Act 2011

Scottish Government
Disclosure Scotland
Transport Scotland
Student Awards Agency for Scotland
Accountant in Bankruptcy
Scottish Agricultural Wages Board
Chief Dental Officer of the Scottish Administration
Chief Medical Officer of the Scottish Administration
Her Majesty's Inspector of Anatomy for Scotland
Her Majesty's Chief Inspector of Prisons for Scotland
Independent Prison Monitors
Prison Monitoring Co-ordinators
Her Majesty's Fire Service Inspectorate for Scotland
Safeguarders' Panel
Drinking Water Quality Regulator for Scotland
Mobility and Access Committee for Scotland

The Keeper of the Records of Scotland

25th July 2022

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 Scottish Government and the other public authorities, listed above, who share a plan in common with the Scottish Government (hereafter referred to as 'The Scottish Government') by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 1st March 2021***.***

The assessment considered whether the RMP of the Scottish Government was developed with proper regard to the 15 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 Scottish Government complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

The **Scottish Government** (Part of the scheduled public authority 'Scottish Ministers') is the devolved government for Scotland which is responsible for most of the issues of day-to-day concern to the people of Scotland, including health, education, justice, rural affairs and transport.

Disclosure Scotland (Part of 'Scottish Ministers') is an Executive Agency of the Scottish Government which provides criminal records checks under Part V of the Police Act 1997 and the Protection of Vulnerable Groups (Scotland) Act 2007.

Transport Scotland (Part of 'Scottish Ministers') is an Executive Agency of the Scottish Government which is responsible for advising Scottish Government on strategy and policy options for transport in Scotland and for increasing sustainable economic growth through the development of national transport projects.

Student Awards Agency for Scotland (Part of ‘Scottish Ministers’) is an Executive Agency of the Scottish Government giving financial support to all eligible students doing a course of higher education in the UK.

Accountant in Bankruptcy (Part of ‘Scottish Ministers’) is an Executive Agency of the Scottish Government responsible for administering the process of personal bankruptcy and recording corporate insolvencies in Scotland.

The **Scottish Agricultural Wages Board** (SAWB) is an executive non-departmental public body set up under the Agricultural Wages (Scotland) Act 1949. The SAWB exists to set minimum rates of pay and other conditions of service for agricultural workers in Scotland.

The **Chief Dental Officer** (CDO) is the Scottish Government’s principal dental adviser, and as such has direct access to ministers. The post has direct involvement in the development of health policy in Scotland, including, health promotion and health protection. The CDO has lead responsibility for issues such as clinical effectiveness, quality assurance, accreditation and research.

The **Chief Medical Officer** (CMO) is the Scottish Government's principal medical adviser and is also Head of the Scottish Medical Civil Service. The post covers every aspect of health in Scotland.

Her Majesty’s Inspector of Anatomy for Scotland inspects premises where bodies for anatomical examination and anatomical specimens are kept. He also inspects record keeping and disposal practices.

Her Majesty's Chief Inspector of Prisons for Scotland is required to inspect the 15 prisons across Scotland in order to establish the treatment of, and the conditions for prisoners and to report publicly on the findings. The Public Services Reform (Inspection and Monitoring of Prisons) (Scotland) Order 2015 came into force on 31 August 2015 and from this date HM Chief Inspector of Prisons for Scotland assumed overall responsibility for the monitoring of prisons, which is carried out on a day to day basis by independent prison monitors.

Independent Prison Monitors appointed under section 7B(2)(a) of the Prisons (Scotland) Act 1989 are volunteers who provide an independent viewpoint on the humane treatment and conditions for prisoners in all prisons across Scotland and conduct investigations either as a result of a prisoner raising an issue or from observations that are made during prison visits. Monitors report formally on their findings.

Prison monitoring co-ordinators appointed under section 7A (2) of the Prisons (Scotland) Act 1989 co-ordinate the work of Independent Prison Monitors.

Her Majesty's Fire Service Inspectorate for Scotland, or HM Fire Service Inspectorate, is an autonomous agency of the Scottish Government. Its function is to provide independent, risk based and proportionate professional inspection of the Scottish Fire and Rescue Service. The Inspectorate can enquire into any matter concerning the operation of a fire and rescue service.

The **Safeguarders Panel** is responsible for recruitment and selection, training, managing appointments, complaints and monitoring performance of safeguarders across Scotland. The statutory responsibility for these functions lies with the Safeguarders Panel which is administered by the Children and Families Directorate.

The **Drinking Water Quality Regulator for Scotland** is responsible for monitoring water quality and enforcing the regulations on behalf of Scottish Ministers. Technical and logistical support is provided by the Drinking Water Quality Division of the Scottish Government.

The **Mobility and Access Committee for Scotland** (MACS) is an advisory non departmental public body. The Convener and Members are appointed by the Minister for Transport. The role of MACS is to consider matters about the needs of disabled persons in connection with transport that the committee think are appropriate and to advise the Scottish Ministers about those matters that the committee think are appropriate.

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 Scottish Government'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

Scottish Government
Disclosure Scotland
Transport Scotland
Student Awards Agency for Scotland
Accountant in Bankruptcy
Scottish Agricultural Wages Board
Chief Dental Officer of the Scottish Administration
Chief Medical Officer of the Scottish Administration
Her Majesty's Inspector of Anatomy for Scotland
Her Majesty's Chief Inspector of Prisons for Scotland
Independent Prison Monitors
Prison monitoring co-ordinators
Her Majesty's Fire Service Inspectorate for Scotland
Safeguarders' Panel
Drinking Water Quality Regulator for Scotland
Mobility and Access Committee for Scotland

(For simplicity the authorities listed above will be referred to as the Scottish Government or 'the SG' throughout this assessment)

Explanation: The Schedule to the Public Records (Scotland) Act includes the umbrella term 'Scottish Ministers'. Several bodies covered by this term are represented in the records management plan being assessed in this report. These are the Scottish Government, Disclosure Scotland, Transport Scotland, the Student Awards Agency for Scotland and the Accountant in Bankruptcy.

However, several other authorities, that are separately scheduled (and therefore are not captured by the term ‘Scottish Ministers’) also share this records management plan ‘in common’. This arrangement is allowed for in the Act under section 1(9) and the Keeper of the Records of Scotland has agreed this is appropriate. These are: The Scottish Agricultural Wages Board, the Chief Dental Officer of the Scottish Administration, the Chief Medical Officer of the Scottish Administration, Her Majesty’s Inspector of Anatomy for Scotland; Her Majesty’s Chief Inspector of Prisons for Scotland; Independent Prison Monitors; Prison monitoring co-ordinators; Her Majesty’s Fire Service Inspectorate for Scotland; the Safeguarders’ Panel; the Drinking Water Quality Regulator for Scotland and the Mobility and Access Committee for Scotland.

Each of the separately scheduled authorities listed above have provided the Keeper with a letter confirming that they are content with this arrangement.

N.B. Since the resubmission of the Scottish Government RMP, HM Inspectorate of Constabulary in Scotland (scheduled under the Act as “Her Majesty’s Chief Inspector of Constabulary and Her Majesty’s Inspectors of Constabulary (appointed under section 33 of the Police (Scotland) Act 1967 (c.77))”) have opted to leave the SG RMP and develop their own. They previously shared a ‘common plan’. The Keeper has agreed this is appropriate and the assessment process for this new, stand-alone, RMP will be underway later in 2022. Therefore, although HMICS is listed in the introduction to the SG RMP, the Keeper’s agreement should not be taken to include that of the HMICS.

Element	Present	Evidence	Notes
1. Senior Officer	G	G	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. The Scottish Government, and the other public authorities noted at the beginning of this assessment (collectively referred to as the SG in this assessment) have identified Lesley Fraser, the Scottish Government's Director General Corporate, as the individual with overall responsibility for records management in the organisation. The identification of the Director General Corporate to this role is supported by the *Records Management Policy* (see element 3), for example under ‘Responsibilities’ (*Policy* page 3). The Director General Corporate is the ‘corporate owner’ of the *Records Management Plan* (the *RMP*). The Director General Corporate is also the SG’s Senior Information Risk Owner (SIRO). The identification of the Director General Corporate as the SG SIRO is supported by the *Data Protection Policy* (see element 9). The Keeper has been provided with the *Roles and Responsibilities* of the SIRO. The *IT Security Policy* (see element 8) also lists the responsibilities of the SIRO: • lead and foster a culture that values, protects and uses information for the public good. • own the overall information risk policy and risk assessment process, test its outcome, and ensure it is used.

			• advise the accountable officer on the information risk aspects of his statement on internal control. Therefore the SIRO is responsible for information risk within the Scottish Government. The role of the SIRO is further explained in the *Scottish Government Information Risk Appetite Statement* (also element 8). The SIRO signed the SG *Information Security Policy Statement* (see element 8) and wrote the foreword to the *Information Asset Owner Handbook* (see Local Records Management under General Comments below). The Knowledge and Information Management (KIM) Branch which is responsible for the *RMP,* the administration of the organisation's electronic records and documents management (eRDM) system (see element 4) and the development and provision of guidance for good records management practice (see element 12) reports directly to the SIRO. The Chief Security Officer, who has direct responsibility for maintaining information security has the right of direct access to the SIRO (see element 8). It is clear that the Director General Corporate/SIRO is suitably aware of the records management provision in the SG. The Keeper agrees that the Scottish Government have identified an appropriate individual to this role as required by the Act.
2. Records Manager	**G**	**G**	The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and that this staff member has

	🟩	🟩	appropriate corporate responsibility, access to resources and skills. The Scottish Government have identified Craig Sclater, Scottish Government Corporate Records Manager, as the individual with day-to-day responsibility for implementing the *RMP*. The identification of the Corporate Records Manager to this role is supported by the *Records Management Policy* (see element 3), for example under ‘Responsibilities’ (*Policy* page 3). It is also supported by the 'Records Management Roles and Responsibilities in Scottish Government' section of *the Records Management Competency Framework* provided to the Keeper. The Corporate Records Manager reviewed and updated the authority’s *RMP*. The Corporate Records Manager reports to the Head of Information Services Operations. It is clear that the identified individual has a detailed knowledge of the records management provision in the authority. The *Scottish Government Assessment and Review Process Statement* provided to the Keeper mentions that reviews will be part of the Corporate Records Manager’s yearly objectives. The Keeper has been provided, separately, with a copy of Mr Sclater’s annual objectives that confirms this. The *Data Protection Act Policy* refers to the SG Data Protection and Information Assets Team'. This group are part of the same wider unit of the SG as the Corporate Records Manager.

			The Keeper agrees that The Scottish Government have identified an appropriate individual to this role as required by the Act.
3. Policy	**G**	**G**	The Act requires an authority to have an appropriate policy statement on records management. The Scottish Government have a *Records Management Policy*. The Keeper has been provided with a copy of this *Policy*. The version supplied to the Keeper has no control sheet and therefore no version number or date. The Records Management Policy is publically available at: https://www.gov.scot/publications/scottish-government-records-management-plan/documents/ . The *Policy* has been approved by the Scottish Government SIRO (see element 1). The *Policy* includes statements that specifically refer to public records not managed on the SG eRDM for example those held on shared drives (limited and principally legacy) and on apps such as Microsoft Teams (for more on records not managed on eRDM see element 4). The Keeper agrees that the *Policy* covers all records, in whatever format, created and held by the SG. The Keeper agrees that the *Records Management Plan* supports the objectives explained in the *Records Management Policy*. The Keeper notes a 'Further Development' against this element: "We are in the process of developing an Information Management strategy which will complement the information provided in our Records Management policy. We plan to finalise this strategy in 2021." The Keeper can confirm that this development has now been achieved and an Information Management Strategy is approved and published at https://www.gov.scot/publications/scottish-government-information-management-

			strategy/ . The Keeper acknowledges that he has been provided with a copy of this new strategy in order that he may keep the Scottish Government submission up-to-date. The Keeper agrees that the Scottish Government has a formal records management policy statement as required by the Act.
4. Business Classification	**G**	**G**	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. The SG recognise this. The *Records Management Policy* (see element 3) states that: "We will maintain a framework of … effective systems related to the core processes of Scottish Government which ensure that evidence of, and information about, its activities and transactions are captured and maintained as viable, accurate and up to date records." and "Our approach to records management is to ensure processes, systems and controls are in place which support the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records." (both quotes from *Records Management Policy* page 2). The vast majority of the public records of the Scottish Government are held on the authority's eRDM (Objective). The eRDM is provided "to give the SG an office wide information and knowledge sharing resource designed to enable efficiencies in the creation, sharing, retention and retrieval of information. It also enables compliance with related legislative requirements for example Freedom of Information Scotland Act (FoISA) and the Data Protection Act (DPA)." (*eRDM Browser Functionality Handbook – see below).* The Keeper is familiar with the functionality of this system (it is the one he uses) and agrees that it suitable for the proper management of public authority records. eRDM applies security classification to all files. Security classification can be used to appropriately restrict access. Classifications are explained in the *Scottish Government Information Risk Appetite Statement* which

	🟩	🟩	has been provided to the Keeper (for more on information security see element 8). The Keeper agrees that the arrangement of records in the SG eRDM system, referred as their ‘file plan’, acts as a business classification scheme for the authority. E-mail records, that are required for business purposes are to be transferred from Outlook to the relevant eRDM folder. The SG provide staff with appropriate guidance on this. For example, the *IT Code of Conduct* (see element 8) sets out guidance on the management of email. E-mail not transferred to eRDM is managed through to permanent destruction in the SG’s Enterprise Vault (see element 6 below and the *Records Management Policy* page 4) All staff are required to be trained on the use of eRDM before accessing the system and have access to an *eRDM Browser Functionality Handbook*. The Keeper agrees that staff have access to this *Handbook* through the SG intranet (‘eRDM and Information Management’ page). The Keeper has been provided with a range of screen-shots showing public records managed on the SG eRDM. Helpfully, these screen-shots include samples of records created by the separately scheduled authorities noted in the explanation above. In line with the Digital First agenda “Realising Scotland’s full potential in a digital world: a digital strategy for Scotland”, https://www.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/ the Scottish Government are digitising their legacy paper files. The contents of each physical file are scanned and stored in an eRDM file. The eRDM file is renamed including the original cipher reference to allow discovery. The programme of digitisation is formally supported in the SG. The *Records*

	🟩	🟩	*Management Policy* (see element 3) which states: “Scottish Government had a purely paper based records management system until 2004. A project is in progress to digitise all paper records (where it is possible to do so) in order to meet with our “digital first” policy. This will ease access to files and vastly reduce the storage space required to hold our legacy material prior to its destruction/transfer to National Records of Scotland in line with the arrangements in our Records Management Plan.” (*Records Management Policy* page 3) The SG *Records Management Policy* also notes that: “Any information created or managed in Microsoft Teams or Office 365 that is a record or documents which are in development and will become a record should be transferred to eRDM.” The creation of public records on apps like Teams is a recently developing issue in the public sector records management community and it is commendable that the SG are recognising the importance of putting policies in place to address this. The Keeper acknowledges that not all documents created by an organisation are a suitable fit for eRDM, for example databases and some templates, and agrees that the SG are very clear on which have been retained on the network drives. The Keeper has been provided with an extract from the Network Drive structure in evidence. The Keeper is also aware that the SG have a backlog of public records, partly in paper format (as noted above) which, although no longer being added to, are yet to be destroyed, transferred to eRDM or transferred to archive (see element 7). The SG have separately explained that they have a bulk import tool available to assist with the transfer of information from shared drives into eRDM. Work on this project was understandably disrupted during the Covid disruption (accessing the paper file store was problematic for example). The Keeper acknowledges that his Archives Depositor Liaison team are actively engaged with the ‘transfer to archive’ section of the project. The SG have provided the Keeper with a project document *Scottish*

	🟩	🟩	*Government Archival Project Analysis and Interim Progress Report* in regard to this project (see element 5 below.) The Keeper is satisfied that records in the ‘Archival Project’ are known and held in a structure that allows them to be discovered as appropriate. **However, they have not yet had proper retention/destruction allocated to them (see element 5).** The SG also operates several stand-alone, line-of-business systems, for example for HR. These line-of-business systems sit outside eRDM, but the Keeper can agree that they are likely to allow the appropriate management of records within a structure as required. The arrangement explained above are supported by evidential documents provided against other elements. For example the *Records Management Policy* (see element 3) or the *Data Protection Act Policy* (see element 9). The *Scottish Government Information Risk Appetite Statement* (see element 8) makes reference to records containing the most sensitive information assets labelled as 'secret' and 'top secret'. The Keeper has been provided with a separate explanation of how these public records are managed and is satisfied that appropriate procedures are in place. The Keeper agrees that the Scottish Government 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.
5. Retention schedule	**A**	**G**	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. The *Records Management Policy* (see element 3) commits the SG to the following

	🟨	🟩	principle "Information and records shall be retained only as long as they are required to support Scottish Government in its business requirements and legal obligations. At the end of that time, the records will either be destroyed or transferred to the National Records of Scotland for permanent preservation. The Scottish Government's retention schedules are the key to effective management of our records, they set out the periods for which particular classes of records are retained in accordance with legal, audit and operational requirements. They provide a formalised, accountable system for the retention and disposal of records, and can help to save time, money and space by ensuring that information is not kept unnecessarily." (*Policy* page 5) The Keeper fully agrees this statement. **For progress against this policy objective see below.** The vast majority of the public records managed by the SG are held on their eRDM system (see element 4). On the issue of assigning retention, the Keeper has been provided with the *Scottish Government Casework File Type Guidance*. The allocation of a record to a file type dictates the retention applied to that record. In the 'Further Development' column against this element the SG state: "We will continue to review our retention and disposal schedules to make sure they continue to meet business needs." (*RMP* page 19). This is a recognition that a retention schedule is a living document, liable to alteration as business needs or updated legislation demands. The Keeper commends this recognition. The Keeper's Assessment Team acknowledges that the SG have provided them with Progress Update Reports (PURs) in 2017, 2018 and 2019 all of which have reported on appropriate adjustment to their *Retention Schedule*. Divisions and Branches in SG draw up their own Branch/Divisional specific retention schedule. Local business areas are also used to review pre-eRDM records as part of the backlog project (see below). The involvement of local areas in the allocation of retention is important and happens automatically in eRDM when local IMSOs

	🟨	🟩	allocate records to file types. (see Local Records Management under General Comments below). The Keeper recognises that not all the public records of the SG are managed on their eRDM and it is important that those records have retention decisions applied to avoid the authority retaining records that have no business use, as noted in the SG policy commitment quoted above. The Keeper can agree that records held on the various business systems (such as eHR) have specified retention decisions allocated and that these are understood. Although the Keeper agrees that the SG can be confident that records on shared drives are structured in such a way that allows them to be discovered, the *RMP* suggests that retention is not yet universally applied. This means that the SG's own policy objectives (quoted at the start of the assessment of this element) are not yet universally achieved. The Keeper is aware that SG are operating with a backlog of public records, partly in paper format, which although no longer being added to are yet to be destroyed, transferred to eRDM or transferred to archive. The Keeper understands (and, from the point of transfer to archive, has been actively involved in) a project has been in place in SG for several years to address this backlog. The *RMP* (page 20) acknowledges the further issue: "At the moment we do not use retention and disposal schedules on shared drives, pst files and public folders. We plan to re-commence our project to review material in these locations and arrange for the material to be disposed of/added to eRDM in line with agreed retention schedules." **The SG have provided the Keeper with the following update regarding the gap in retention noted above: "In terms of our legacy paper records these will all continue to be managed in line with the arrangements stated in the document titled 'Scottish Government Paper Records Retention schedule pre-eRDM'. We**

	🟨	🟩	**continue to progress the project to digitise our paper records in line with the document titled ‘Digitisation of Legacy Paper Files’.** **We have this year [2022] commenced a Shared Drive Programme which will firstly see content held in ‘H Drives’ be reviewed by each individual member of staff and either added to the appropriate eRDM file where it is part of the corporate record (this exercise is to be completed by the end of July 2022) or deleted where it has no/no longer has any business value (note: any deletion of corporate information will be done in consultation with our branch). Following this we will begin the task of tackling content held on the G drive, pst files and public folders whereby business areas will be asked to review material and add any content which is for the corporate record to eRDM unless there is a valid business reason why it cannot be stored there (e.g. databases) or alternatively delete information which has no/no longer has any business value (as above any deletion of corporate information will be done in consultation with our branch). On completion of this exercise (which will inevitably take a reasonable period of time to complete) the vast majority of information for the corporate record will be stored in eRDM (where it will be managed appropriately in line with our RMP arrangements) and those objects not stored in eRDM (e.g. databases) will be recorded as Information Assets by local Information Asset Owners which will ensure they can be appropriately managed (note: we continue to advise business areas to ensure that regular ‘snapshots’ or reporting outputs of their databases are stored in eRDM to maintain the corporate record).”** **Considering this statement, the Keeper accepts that the SG recognise that retention is not yet satisfactorily applied to all public records, but he is satisfied that there is a clear methodology in action to resolve the issue while sensibly weeding-out records that are of no ongoing business value. The Keeper also notes that the project to digitise paper records is in line with the**

	🟨	🟩	**SG's Digital First agenda.** **The Keeper can agree this element of the Scottish Government's *RMP* on improvement model terms. This means that the authority has identified a gap in their records management provision (there is a backlog of legacy records that do not have retention/destruction processes applied) and have put processes in place to close that gap. The Keeper's agreement will be conditional on his being kept up-to-date with progress.**
6. Destruction Arrangements	**G**	**G**	The Act requires that public records are destroyed in a timely, controlled and secure manner. The Scottish Government acknowledge this and it is their formal policy that "Our approach to records management is to ensure processes, systems and controls are in place which support the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and **disposal of records**." and a policy commitment that they will "dispose of records that are no longer required in an appropriate manner" (*Records Management Policy* – see element 3 - 'Objectives' page 2). With this commitment in mind, the SG has the following process in place for the destruction of their public records: Digital (eRDM): Records are automatically deleted according to the retention applied (see element 5) and a 'stub' retained as evidence of destruction. This acts as a destruction log and is to be commended as best practice. The Keeper has been provided with a screen-shot from the SG eRDM showing a sample of destroyed file information. E-Mail: The Scottish Government use Enterprise Vault to manage e-mail from all

			mailboxes. This ensures that e-mails are either transferred to the eRDM folder structure or automatically destroyed. The Keeper is familiar with the functionality of Enterprise Vault and agrees it is a suitable method for guaranteeing the appropriate controlled, secure and irretrievable destruction of e-mail. Paper: Hard-copy records are destroyed by a third-party shredding company. The Keeper has been provided with a sample destruction certificate as evidence that this arrangement is operational. Hardware: Destruction of hardware is controlled through the use of a third-party. The Scottish Government maintain a list of all assets passed for destruction and receives a certificate of destruction detailing all equipment that has been destroyed. Again the Keeper has been provided with sample destruction certificate as evidence that this arrangement is operational. Back-Ups: The SG, quite properly, keep back-ups of public records for business continuity purposes (see element 10). It is important that an authority understands the availability of back-up copies beyond the destruction of the original. The Keeper has been provided with the following statement: “The Scottish Government do daily incremental backups and then at the weekend full back ups are taken of the system. The backups are then kept for four weeks and are then destroyed and the information then becomes irretrievable.” He has also be provided with an explanation of the back-up process in eRDM. The Keeper agrees that the Scottish Government has processes in place to irretrievably destroy their records when appropriate.
7. Archiving and Transfer	**G**	**A**	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.

	🟩	🟨	The Scottish Government has identified the National Records of Scotland (NRS) as the repository to which they will transfer the selection of their public records that have been categorised as suitable for permanent preservation. The SG *Records Management Policy* (see element 3) supports this arrangement: "We will ensure the effective transfer of Scottish Government records to the National Records of Scotland (NRS) which are selected by them for permanent preservation." (*Policy* page 2) and "Information and records shall be retained only as long as they are required to support Scottish Government in its business requirements and legal obligations. At the end of that time, the records will either be destroyed or transferred to the National Records of Scotland for permanent preservation" (page 5). 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 *Supplementary Guidance on Proper Arrangements for Archiving Public Records*: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/supplementary-guidance-on-proper-arrangements-for-archiving-public-records.pdf The Keeper acknowledges that this arrangement is operational and public records of the SG are routinely transferred into NRS. **However, the Service Level Agreement under which these arrangements operate is out-of-date. The NRS Client Management Team and the Corporate Records Manager (see element 2) have both acknowledged this discrepancy and have set up a meeting to begin taking forward the updating of these documents. The SG have also committed to provide the Keeper with a copy of the updated agreement as soon as it becomes available.**

	🟩	🟨	The Keeper acknowledges that the SG have provided him with a copy of the up-to-date *NRS Depositor Guidance for the Transfer of Archival Born Digital Records*. The Keeper notes that, under the ‘Further Development’ column against this element, the SG state: “The NRS selection policy and SG iTECS-NRS Service Level Agreement will be reviewed and updated in 2021 in conjunction with NRS.” (*RMP* page 24). **The Keeper can agree this element of the SG RMP under ‘improvement model’ terms. He can do this when he is convinced that, having identified a gap in records management provision, an authority has put appropriate process in place to close that gap.**
8. Information Security	**G**	**G**	The Act requires that public records are held in accordance with information security compliance requirements. The Scottish Government "understand that information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption." (*IT Security Policy* section 3.1.3 – see below). They commit that “Information will be protected against unauthorised access” (*Information Security Policy Statement* – also below) and note that “The delivery of efficient public services, including the proper protection of citizen data, requires modern and functional technology. Resilience to cyber threats, compliance with data protection laws [see element 9] and management of national security-related information within these systems will require security to be integral to their design and implementation.” (*IT Security Policy* section 1.1). The SG operates an information security framework supported by an *Information Security Policy Statement* and specifically endorsed and described in an *IT Security*

	🟩	🟩	*Policy*. Both the *Statement* and the *Policy* have been supplied to the Keeper and are available to SG staff through their intranet (IT and Information Management page). The *IT Security Policy* is v1.0, March 2020. The Keeper agrees that the *Scottish Government Information Security Policy Statement* includes reference to physical records, removable media and reporting. The *IT Security Policy* also provides guidance around a range of security issues including physical security, remote working and e-mail and explains the procedures for the reporting of incidents (the SG has a Security Incident Reporting Tool). It also emphasises the potential security risks around change (for example section 4.3.1). The *Policy* is mapped against the standards of the UK *Security Policy Framework: Protecting Government Assets* [Security policy framework: protecting government assets - GOV.UK (www.gov.uk)](https://www.gov.uk). The information security framework is populated with a suite of policies and guidance covering a range of information security issues. A selection of these have also been shared with the Keeper (for example the *Clear Desk Policy or Data Handling Standard or IT Code of Conduct*). Guidance documents include guidance on the reporting of security incidents, actual or potential. The Keeper agrees that these policy and guidance documents and other useful security information (for example *'Home working security: Your responsibilities*') are available on the SG intranet. The Director General Corporate (see element 1) is the SG's Senior Information Risk Owner (SIRO). The *Information Security Policy Statement* notes that the Chief Security Officer, who has direct responsibility for maintaining the *Policy*, providing advice and guidance on its implementation, has the right of direct access to the SIRO.

			The SG SIRO is responsible for information risk and advises on the effectiveness of information risk management across the Organisation. The SG have shared the details of their risk assessment procedures, and guidance on how to populate/review their risk register, with the Keeper. This includes the *SG Risk Strategy and Policy*, the *SG Information Risk Management Appetite Statement* and the *SG Risk Management* Guide. The Keeper agrees that the Scottish Government have procedures in place to appropriately ensure the security of their records as required by the Act.
9. Data Protection	**G**	**G**	The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law. The Scottish Government is registered as a data controller with the Information Commissioner's Office (ICO): Z4857137 [Information Commissioners - Data protection register - entry details (ico.org.uk)]() (they are part of 'Scottish Ministers') The SG have a *Data Protection Policy*. The Keeper has been provided with a copy of this *Policy*. This is version 1.0 (undated). The *Data Protection Policy* confirms that "The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 impose obligations on the use of all personal data held by the Scottish Government, whether it relates to data subjects and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation, defined as data subjects." (*Data Protection Policy* section 1) The *Data Protection Policy* goes on to properly explain the 6 principles of data protection (section 3) and provides guidance to staff on reporting incidents (section

	🟩	🟩	4). The SG web page [Request information - gov.scot (www.gov.scot)](https://www.gov.scot) provides helpful information and the following link provides the public with information regarding how they can make a subject access request https://www.gov.scot/publications/subject-access-request-form/ There is also a privacy notice published at https://www.gov.scot/privacy/ The Keeper notes that SG staff have been issued with appropriate guidance regarding the processing of subject access requests. The SG have appointed a Data Protection Officer as required by the Data Protection Act 2018. The Keeper has been provided with data protection supporting documents such as *Data Sharing Agreement Templates* (see element 14) and, as noted above, *Subject Access Request Guidance*. The Keeper agrees that staff can access relevant data protection information, including the *Policy* and *Data Protection Impact Assessments* from the SG intranet. The SG has a mandatory, annual, e-learning data protection training programme (see element 12). The *IT Security Policy* and the *IT Code of Conduct* (both see element 8) support data protection arrangements in the SG. The Keeper agrees that the Scottish Government have arrangements in place that allow them to properly comply with data protection legislation.

10. Business Continuity and Vital Records	**G**	**G**	The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning. The Scottish Government recognise this. They commit that "Business Continuity Plans will be produced, maintained and tested." (*Information Security Policy Statement*). The SG have a further policy commitments that they will "protect vital records" (*Records Management Policy* - see element 3 - page 2) and that "The Scottish Government shall...know and record...The impact of loss of availability of the service" and "The Scottish Government shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise " (*IT Security Policy* sections 3.3.1 and 7.1). The SG commit that record recovery procedures (see element 10) will be tested annually: "The Scottish Government shall identify and test contingency procedures to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service, and shall…rehearse response and recovery plans at least annually. Restoring the service to normal operation should be a well-practised scenario." (*IT Security Policy* section 7.1.1). Record recovery in the SG is dependent on which system the record is managed (see element 4). The vast majority of the public records of the Scottish Government are held on the authority's eRDM (Objective). Back-ups are simultaneously replicated at a disaster recovery centre based outside Edinburgh. In event of a disruption to the service in the Edinburgh data centre, the SG IT systems automatically switch to use the back-up disaster recovery data centre. Digital records held outwith the eRDM are backed-up from the network drives.

	🟩	🟩	These back-ups are daily with full back-ups of the entire 'Scots' system taken over the weekend. Scots back-ups are then kept for four weeks and are then destroyed and the information then becomes irretrievable. No physical backup copies of electronic data are taken and stored, for example on magnetic tapes or CDS, and no SG electronic data is stored outside the main and back-up servers. Paper Records (see element 4): Under the Scottish Government's Digital First agenda the SG are digitising their paper records which will eliminate the risk of hard-copy records being damaged/ destroyed as a result of the likes of a fire/flooding. The SG have instigated a rigorous evaluation process to ensure their paper storage facility is fit for purpose including regular site visits. The Keeper agrees that the Scottish Government have an approved and operational business continuity process and that information management and records recovery properly feature in the authority's plans.
11. Audit trail	**G**	**G**	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. The Scottish Government recognise this and state "our information needs to be found quickly and easily and this saves on resources, staff time and effort looking for lost documents." (*eRDM Browser Functionality Handbook* – see below) With this in mind, the SG have the following processes in place. (For the structure of the Scottish Government records management systems see element 4 above.) Digital eRDM: The vast majority of the public records of the Scottish Government are managed on the eRDM. The Objective system has a powerful search facility that

	🟩	🟩	allows a user to track all records using a variety of search criteria including metadata. The efficiency of the search facility relies on consistent naming of documents as they are saved as records on the system. Each change to a record in eRDM is recorded automatically by the system. Staff are also encouraged to use version control v0.1, v0.2, v1.0 etc. to create different documents to, at least temporarily, allow previous draft versions to be consulted to help understand the development of a document. In theory locating the most recent version of a record should be straightforward in eDRM. The SG has a *eRDM Browser Functionality Handbook* which has been provided to the Keeper. The Keeper agrees that this gives clear and appropriate instructions to staff to ensure that records are named on the eRDM in such a way as will allow tracking. Digital Line-of-Business: The Scottish Government operate line-of-business systems such as for HR or iFix (IT request system). The Keeper can accept these systems have record tracking and version control functionality. Digital Shared Drives: Public records still held on corporate shared drives have been located and identified. The Keeper has been provided with Scottish Government Archival Policy for Shared Drives. It is not possible to automatically track every change to a document on a shared drive. The SG understand this lack of provision and the Keeper recognises that they are phasing out the use of shared drives under a structured and agreed programme of improvement. Hard-Copy Records: The *RMP* (page 33) states: “Paper records are identified within the Legacy Paper File database. The database tracks the movement (including those passed to NRS for permanent preservation) and destruction of files. As mentioned previously we are in the progress of digitising our legacy paper records

			which will allow us to capture them in eRDM [see element 4]". The Keeper has been provided with a screenshot Extract from Legacy Paper Filing system as evidence that paper files can be tracked prior to undergoing the process explained above. The SG paper files are no longer being added to or amended. The Keeper is satisfied that all the public records of the SG are able to be located and correctly identified notwithstanding that work is still underway to ensure that retention/destruction/archiving decisions are applied. There is no suggestion in the *RMP* that the SG is unsure the are able to discover records that fall into this category. Therefore, the Keeper agrees the Scottish Government has procedures in place that will allow them to locate their records and assure themselves that the located record is the correct version.
12. Competency Framework for records management staff	**G**	**G**	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported. The Scottish Government has commitment that "All Scottish Government staff receive training so they are aware of their responsibilities as individuals with respect to record keeping and management and to ensure they are competent to carry out their designated duties. This includes online training in the use of the eRDM system which is then complemented by organisational policies and procedures and guidance documentation." (*Records Management Policy* page 5). The Scottish Government state: "Core competencies, key knowledge and skills required by staff with responsibilities for Records Management have been clearly defined within the Records Management Competency Framework. This ensures that staff understand their roles and responsibilities and can offer expert advice and guidance." (*RMP* page 35) (see also Local Records Management under General

	🟩	🟩	Comments below). The Keeper has been provided with a copy of the *Records Management Competency Framework*. The *Competency Framework* states that the Corporate Records Manager “will be professionally qualified in information/records management or working towards such a professional qualification.” Craig Sclater has attended a number of records management courses and events which have attracted a certificate of competence following completion of the training and coursework. Therefore it is clear that Mr Sclater is ‘working towards a professional qualification’. The *RMP* page 35 commits the SG as follows “We will also endeavour to have all staff in our Records Management team undertake appropriate records management courses to enhance their knowledge and understanding of the subject.” Considering that the *RMP*, and therefore this commitment, has be approved by the Director General Corporate and SIRO (see element 1), the Keeper welcomes this statement. The Knowledge and Information Management (KIM) Branch is responsible for…the development and provision of guidance for good records management practice.” (*Records Management Policy* – see element 3 - page 3). They are assisted by local records management IMSOs (see local Records Management below). The SIRO (see element 1) has a policy responsibility for ensuring “that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work”. (*Scottish Government IT Security Policy* – see below - 3.1.2.2.) All staff are required to complete training on the use of eRDM before they are able to access the system and going forward have access to an *eRDM Browser Functionality Handbook* (see element 4). This document is vital guidance for all aspects of using eRDM from managing e-mails to changing the colour scheme. The Keeper agrees that staff have access to this handbook through the SG intranet

	🟩	🟩	(eRDM and Information Management page). All staff must be trained before they can handle personal information in any form in the course of their job. (*Data Protection Policy* - see element 9 - section 5) With this in mind, all staff are required to complete “Data Protection” and “Responsible for Information – General User’” e-learning training on an annual basis. In addition to completing the “Responsible for” course, all staff are provided with guidance concerning the procedures and considerations for electronic and hard copy distribution of information (*RMP* page 39). Guidance is available on the SG intranet and SG ‘Learning Portal’. The Keeper has access to this guidance and agrees it is appropriate. The Keeper has been provided with details of training modules in evidence (such as ‘Managing Information’). The SG have made a commitment that "Information security training will be available to all staff." This commitment appears in the *Scottish Government Information Security Policy Statement*, dated 2015 and signed by Senior Information Risk Owner (SIRO) at the time. This is supported by a policy objective in the *Scottish Government IT Security Policy* “that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.” Both the *IT Policy* and the *Statement* have been provided to the Keeper in evidence (see element 8). “Security mandatory training must be completed by all staff and shall also be encouraged to complete any recommended security learning.” (*Scottish Government IT Security Policy* section 3.1.2.4) See element 8 for Information

			Security. “The Scottish Government shall maintain employee awareness of the Scottish Government’s expectations of them during an emergency or business continuity threatening situation.” (*Scottish Government IT Security Policy* section 7.1.1) See element 10 for Business Continuity. The SG RM Team are also in the process of requesting approval for Records Management Team staff to be recognised in the Digital, Data and Technology profession. They have committed to update the Keeper on this matter when appropriate. 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 also agrees that the Scottish Government consider information governance training for other staff as required.
13. Assessment and Review	**G**	**G**	Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review. The RMP is reviewed annually. Reviewing the implementation of the *RMP* is the responsibility of the Corporate Records Manager (see element 2). The results of any review are reported to the iTECS Senior Leadership Team and the Senior Information Risk Owner. The SG have provided the Keeper with the following statement in their evidence pack: “We are committed to completing the Records Management Plan Progress Update review on an annual basis (excluding years we are required to re-submit our

	🟩	🟩	Records Management Plan to the Keeper of the Records for approval). The outcome of this review will be shared with the iTECS Senior Leadership Team and the Senior Information Risk Owner in order that they are aware of progress which has been made and weaknesses that require to be addressed. This review will be part of the Corporate Records Manager's yearly objectives." (*Scottish Government Assessment and Review Process Statement*) Separately from the submitted *RMP*, the SG have made the following statement about the methodology of review which the Keeper acknowledges: "A review of corporate information management in SG was published in June 2021. This has led to a major information governance programme of work which has strengthened the information governance roles in the organisation. We have introduced an annual Certificates of Assurance process and an Information Management Maturity Assessment benchmarking exercise was undertaken at the beginning of 2022 but in future years the questions from that Maturity Assessment will form part of the Scottish Government annual Certificates of Assurance process. Directorates will need to assure themselves they are confident that all information within their areas is managed appropriately and in line with current policies and procedures." The Keeper notes that a methodology for annual reporting on information security is in place: "[IOAs] understand and address risks to the information, ensure that information is fully used within the law for the public good, and provide written input to the senior information risk owner annually on the security and use of their asset." (*IT Security Policy* – see element 8 – section 3.1.2.3) The *RMP* (page 16) commits the SG to an annual review of their *Business Classification Scheme* (see element 4) and to review the *Records Management Policy* (see element 3) in order to ensure that it continues to reflect the organisational position in relation to record keeping.

	🟩	🟩	Furthermore, the SG have committed to reviewing their information security framework documents and business continuity planning (see elements 8 and 10) “regularly and updated as required”. The *Information Security Policy Statement* itself will be reviewed annually under the direction of the Chief Security Officer (*Scottish Government Information Security Policy Statement* section 8)) The *Data Protection Act Policy* (see element 9) is to be reviewed annually (*DP Policy* section 1). The SG commit that reviews of access permissions (see element 8) will be carried out (*IT Security Policy* section 4.1.5). The SG commit that record recovery procedures (see element 10) will be tested annually: “The Scottish Government shall identify and test contingency procedures to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service, and shall…rehearse response and recovery plans at least annually. Restoring the service to normal operation should be a well-practised scenario.” (*IT Security Policy* section 7.1.1). The SG has committed to updating the *Information Risk Appetite Statement* when required (se element 8) (*Information Risk Appetite Statement* section 1). The current *Information Risk Appetite Statement* is dated from 2021 **However, the Keeper would like to note that several evidence documents provided to him have no control sheet attached. Therefore, he is not able to judge who authorised them, their approval date or when they are due to be reviewed.** As noted in the *Statement* above, the SG intend to use the voluntary Progress Update Review (PUR) reporting methodology that was developed by his PRSA

			Assessment Team in conjunction with stakeholders. This is a welcome commitment. The Assessment Team acknowledges that the SG have already engaged with this process and will ensure that they will continue to be supplied with a template for this process annually. The Keeper agrees that the Scottish Government have made a firm commitment to review their *RMP* as required by the Act and have explained who will carry out this review and by what methodology.
14. Shared Information	**G**	**G**	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. The Scottish Government shares information with third parties and does so using data sharing templates. One template is for sharing personal information (the *RMP* – page 39 – specifically states that data sharing in compliant with data protection guidance – see element 9) and another template for the sharing of data that does not include personal information. Both these templates have been provided to the Keeper in evidence. The Keeper agrees that these templates include appropriate guidance for staff against each section. The Keeper agrees that SG staff have access to these templates through the SG intranet (Information Sharing Tools page). The Keeper has also been provided with a sample agreement (with the Scottish Fire and Rescue Service) as evidence that the templates are currently operational. The principle information sharing tool utilised by the SG is the collaboration platform Objective Connect. The Keeper is familiar with this system and agrees it is appropriate for the sharing of public records. SG Staff are introduced to this system

			in the *eRDM Browser Functionality Handbook* (see element 4) for example at section 23. In addition to completing the “Responsible for Information – General User” training (see element 12), SG staff are provided with guidance on the procedures for information sharing. The SG state that “Where information assets are shared with suppliers, it is important that the risk stance is articulated to them, including expectations on how risks are managed.” (*Scottish Government Information Risk Appetite Statement –* see element 8 – section 01) The Keeper can agree that the Scottish Government properly considers records governance when undertaking information sharing programmes.
15. Public records created or held by third parties	**G**	**G**	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. The Scottish Government and some of those separately scheduled authorities noted in the ‘Explanation’ above, contract some of their functions to third parties. For example, the SG currently contracts management of the national Safeguarders Panel to Children 1st For the SG, contracts which contain details of what should happen to information that they produce are provided on the SG website. All information relating to procurement contracts awarded by SG can be found at the following link **https://www.gov.scot/publications/terms-and-conditions-for-scottish-government-contracts/**

	🟩	🟩	The SG have provided the Keeper with the *Scottish Government Model Framework Agreement Terms and Conditions*. The Keeper agrees that that the template framework document includes information governance clauses such as data protection (section 14); freedom of information and transparency (section 15); Audit and Records Management (section 18) and exit management (section 44). An example that shows records management is properly considered when contracting out functions to third parties is: “At the end of the Framework Agreement, the Contractor shall transfer the records in question to the Authority, such transfer to include full ownership of the records including all Intellectual Property Rights in relation thereto. The transfer shall be at no cost to the Authority. The Contractor shall ensure that all relevant information reasonably required to locate individual items within the records, including metadata and database schema, are also offered to the Authority on the same terms.” (*Model Framework Agreement Terms and Conditions* section 18.5). The *Model* specifically mentions responsibilities under the Public Records (Scotland) Act 2011. The SG *IT Security Policy* and *Information Security Policy Statement* (see element 8) specifically make reference to third-party contractors and service providers. For example “Third parties and suppliers may be required to adopt the same risk appetite and security controls.” (*Statement* and in the *IT Security Policy* section 4). The Keeper agrees that the Scottish Government has properly considered the management of records created by third parties while they undertake activities in pursuance of functions of the SG under contract.

Scottish Government
Disclosure Scotland
Transport Scotland
Student Awards Agency for Scotland
Accountant in Bankruptcy
Scottish Agricultural Wages Board
Chief Dental Officer of the Scottish Administration
Chief Medical Officer of the Scottish Administration
Her Majesty's Inspector of Anatomy for Scotland
Her Majesty's Chief Inspector of Prisons for Scotland
Independent Prison Monitors
Prison monitoring co-ordinators
Her Majesty's Fire Service Inspectorate for Scotland
Safeguarders' Panel
Drinking Water Quality Regulator for Scotland
Mobility and Access Committee for Scotland

(For simplicity the authorities listed above will be referred to as the Scottish Government or 'the SG' throughout this assessment)

Explanation: The Schedule to the Public Records (Scotland) Act includes the umbrella term 'Scottish Ministers'. Several bodies covered by this term are represented in the records management plan being assessed in this report. These are The Scottish Government, Disclosure Scotland, Transport Scotland, the Student Awards Agency for Scotland and the Accountant in Bankruptcy.

However, several other authorities, that are separately scheduled (and therefore are not captured by the term 'Scottish Ministers') also share this records management plan 'in common'. This arrangement is allowed for in the Act under section

1(9) and the Keeper of the Records of Scotland has agreed this is appropriate. These are: The Scottish Agricultural Wages Board, the Chief Dental Officer of the Scottish Administration, the Chief Medical Officer of the Scottish Administration, Her Majesty's Inspector of Anatomy for Scotland; Her Majesty's Chief Inspector of Prisons for Scotland; Independent Prison Monitors; Prison monitoring co-ordinators; Her Majesty's Fire Service Inspectorate for Scotland; the Safeguarders' Panel; the Drinking Water Quality Regulator for Scotland and the Mobility and Access Committee for Scotland.

Each of the separately scheduled authorities listed above have provided the Keeper with a letter confirming that they are content with this arrangement.

N.B. Since the resubmission of the Scottish Government RMP, HM Inspectorate of Constabulary in Scotland (scheduled under the Act as Her Majesty's Chief Inspector of Constabulary and Her Majesty's Inspectors of Constabulary (appointed under section 33 of the Police (Scotland) Act 1967 (c.77))) have opted to leave the SG RMP and develop their own. They previously shared a 'common plan'. The Keeper has agreed this is appropriate and the assessment process for this new, stand-alone, RMP will be underway later in 2022. Therefore, although HMICS is listed in the introduction to the SG RMP, the Keeper's agreement should not be taken to include that of the HMICS.

General Notes on submission:

This assessment is on the *Records Management Plan* (the *RMP*) of the Scottish Government, in common with the other authorities indicated above, as submitted to the Keeper of the Records of Scotland (the Keeper), for his review and agreement, in September 2021.

A previous version (2017) of the *RMP* is publically available at: https://www.gov.scot/publications/scottish-government-records-management-plan/

This is the second formal records management plan received from the Scottish Government by the Keeper. The first was agreed on the 20th August 2015: Scottish Government Assessment Report (nrscotland.gov.uk)

The Scottish Government *RMP* follows the 15 element structure of the Keeper's *Model Plan*: Model Records Management Plan | National Records of Scotland (nrscotland.gov.uk)

The Scottish Government *RMP* specifically mentions compliance with the Public Records (Scotland) Act 2011.

The SG states: "The Scottish Government recognises that its records are an important public asset and are a key resource in the effective operation, policy making and accountability of Scottish Government. Like any asset, records require careful management …." (*Records Management Policy* – see element 3) Introduction. The Keeper welcomes this recognition.

The *RMP* also states (page 13): "Scottish Government is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal or archive. This approach ensures that Scottish Government can:

- control the quality, quantity and security of the information that it generates;
- maintain the information in an effective manner whilst ensuring compliance with our legislative requirements ."

The Keeper agrees this overarching statement.

Local Records Management:

The Scottish Government have set up Information Asset Owners (IAOs) in local business areas. The *IT Security Policy* (see element 8) lists their responsibilities as follows:

"IAOs are senior individuals who understand what information is held, what is added and removed, how information is moved, and who has access and why.
They understand and address risks to the information, ensure that information is fully used within the law for the public good, and provide written input to the senior information risk owner annually on the security and use of their asset :

- lead and foster a culture that values, protects and uses information for the public good.
- knows what information the asset holds, and what enters and leaves it and why.
- knows who has access and why, and ensures their use of it is monitored.
- understands and addresses risks to the asset, and provides assurance to the SIRO.

- ensures the asset is fully used for the public good, including responding to requests for access from others.”

(IT Security Policy section 3.1.2.3)

IAOs also have a responsibility to ensure compliance with data protection law within their business area (see element 9) and to ensure that the correct security labelling is applied to the information for which they are responsible.

The appointment of IAOs is a requirement of the organisation’s *Information Risk Appetite Statement* (for example section 3.1). Where business areas operate with a risk tolerance outside their normal local risk appetite, the IAO is required to record this.

It is one of the responsibilities of the SIRO (see element 1) to ensure that each "department has IAOs who are skilled, focussed on the issues, and supported, plus the specialists that it needs."

In order to carry out their duties the IAOs are assisted by Information Management Support Officers (IMSOs). Each business area in the SG has one of these local records management champions who are specially trained on the use of eRDM and have extra administrative permissions on the system. They are also responsible for providing advice to their local business teams and to promote good record keeping in their areas.

The *Records Management Policy* (see element 3) states: “Information Management Support Officers (IMSOs), who are nominated by the business area, and provide a key point of contact between business areas and the KIM [Knowledge and Information Management] Branch. IMSOs have a vital role in ensuring that records are maintained and disposed of in accordance with Scottish Government’s published retention policies. They also advise local business teams and promote good record keeping in their areas.” (*Records Management Policy* page 3).

The *RMP* (page 37) notes that “Each of the policies and procedures produced in line with the requirements of the Public Records (Scotland) Act 2011 have been created in consultation with colleagues across the organisation.” This is to be commended.

Managers are directly responsible for implementing the *Information Security Policy* within their business area and any third parties undertaking work on behalf of that business area (see element 8) (*Information Security Policy Statement* and *IT Security Policy* section 1.2).

“Access shall be removed when individuals leave their role or the organisation. Line managers are responsible for ensuring that this is carried out.” (*IT Security Policy* section 4.1.5)

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 Scottish Government. Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development are:

5. Retention schedule
7. Archiving and Transfer

7. Keeper’s Determination

Based on the assessment process detailed above, the Keeper **agrees** the RMP of The Scottish Government.

- The Keeper recommends that the Scottish Government 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,

E. Course

…………………………………… …………………………………

Pete Wadley
Public Records Officer

Liz Course
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 Scottish Government In agreeing this RMP, the Keeper expects the Scottish Government to fully implement the agreed RMP and meet its obligations under the Act.

……………………………………………

Paul Lowe
Keeper of the Records of Scotland