National Records of Scotland

Public Records (Scotland) Act 2011

Public Health Scotland

The Keeper of the Records of Scotland

2nd August 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 Public Health Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 12th July 2021.

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

3. Authority Background

Public Health Scotland is Scotland's lead national agency for improving and protecting the health and wellbeing of all of Scotland's people.

Their vision is for a Scotland where everybody thrives. Focusing on prevention and early intervention, they aim to increase healthy life expectancy and reduce premature mortality by responding to the wider determinants that impact on people's health and wellbeing. To do this, they use data, intelligence and a place-based approach to lead and deliver Scotland's public health priorities.

Public Health Scotland are jointly sponsored by COSLA and the Scottish Government and collaborate across the public and third sectors. They provide advice and support to local government and authorities in a professionally independent manner.

The values of respect, collaboration, innovation, excellence and integrity is at the heart of their work.

Public Health Scotland

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 Public Health Scotland’s RMP was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

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

5. Model Plan Elements: Checklist

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. Public Health Scotland (PHS) have identified Angela Leitch, Chief Executive Officer, as having overall strategic responsibility for records management in the organisation. This is supported by a *CEO Covering Letter* (dated 30 June 2021). It identifies Angela Leitch as the CEO and states her commitment to ensuring PHS manage their records appropriately and in compliance with legislation. It also notes PHS's commitment to the continuing development of records management provision as the organisation develops. The leadership in records management was previously delegated to the post of Director of Strategic Planning and Performance and is now (as of May 2022), following organisational change, delegated to Scott Heald, Director of Data and Digital Innovation. The *RMP* carries the signed endorsement of Mr Heald and also states his endorsement of the *Records Management Policy*. The *Staff Governance Committee Minutes June 2021*, show the endorsement of the approval of the *Records Management Policy* and that both the Chief Executive and Director of Strategic Planning and Performance (post previously delegated to lead

	🟩	🟩	records management) were in attendance. The Keeper agrees that Public Health Scotland 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 has appropriate corporate responsibility, access to resources and skills. Public Health Scotland have identified Duncan Robertson, Senior Policy, Risk and Deputy Data Protection Officer as their appointed Corporate Records Manager holding responsibility for implementing the RMP and list his responsibilities, including ensuring statutory and regulatory compliance and developing and co-ordinating records management in the organisation. A *Job Description Senior Policy, Risk & Data Protection Officer* (dated 2018 and from predecessor body, NHS Health Scotland) has been provided. It has been confirmed separately that an updated PHS job description for the role is currently being developed and approved. The *Job Description* outlines responsibilities for information governance, records management and compliance with legislation, including PRSA. It confirms the role involves regular contact with the Chief Executive's Office. It notes that it is the responsibility of the post holder to establish an Information Management Group (this is also mentioned on page 23 of the *RMP*, see element 13 for further comments). PHS have confirmed separately that an Information Governance Board has been established and the first meeting took place on 30th March 2022. The Board's remit includes records management. The Board reports to the Senior Leadership Team and the Public Health and Wellbeing Committee. **The Keeper would welcome sight of the terms of reference for the IG Board and confirmation of the frequency of meetings when available.**

			As noted under element 1, the leadership of records management is delegated to the Director of Data and Digital Innovation. PHS have confirmed separately that the Senior Policy, Risk and Deputy Data Protection Officer will report on PHS Records Management to the Director of Data and Digital Innovation. The Senior Policy, Risk and Deputy Data Protection Officer achieved the Practitioner Certificate in Scottish Public Sector Records Management in February 2021. A copy of this certificate has been supplied. The Senior Policy, Risk and Deputy Data Protection Officer is the author of the *RMP; Records Management, Document Storage and Retention Policy;* and edited the *Data Protection Policy*. The Keeper agrees that Public Health Scotland 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. Public Health Scotland have a combined *Records Management, Document Storage and Retention Policy (RMDSR Policy)*. The Keeper has been provided with a copy. This is version 2.0, approved on 2 June 2021. This policy will be reviewed every two years, or sooner if required, with the next review planned for June 2023. Public Health Scotland recognise that ''records are its corporate memory, providing evidence of actions, decisions and representing a vital asset to support its daily functions and operation.'' and ''They support continuity, accountability, efficiency and productivity and help deliver its services in consistent and equitable ways.'' (*RMDSR Policy* page 3)

	🟩	🟩	The *RMDSR Policy* was approved by the Staff Governance Committee in June 2021. (see element 1) The *RMDSR Policy* outlines its scope, application and lists eight statements on the management of records within PHS which cover: compliance; accountability; quality; accessibility; security; retention and disposal; training; and performance and measurement. The *RMDSR Policy* (page 2) states it ''applies to all PHS staff and those working on behalf of PHS at any location.'' The Keeper agrees that the *RMP* supports the objectives of the *RMDSR Policy*. The *RMDSR Policy* is accessible to staff via the staff intranet site and a screenshot has been provided showing this. The Keeper notes the intention to publish the Policy on the PHS website. **There is an action noted to develop further supporting documentation, ''detailed procedures for electronic records to be developed as M365/Sharepoint is introduced across Public Health Scotland'' and ''a single PHS approach to management of paper records''. The Keeper would like to be informed as this work progresses. The Progress Update Review (PUR) reporting mechanism, Progress Update Reviews | National Records of Scotland (nrscotland.gov.uk) can be used for such updates.** The Keeper agrees that Public Health Scotland has a formal records management policy statement as required by the Act.

4. Business Classification	**A**	**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. Public Health Scotland recognise ‘‘It’s essential to capture, manage and preserve information in an organised system.’’ And that ‘‘Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of staff time and physical and electronic space through co-ordination of information and storage systems.’’ (*RMDSR Policy* pages 2-3) Public Health Scotland commit to ensuring ‘‘records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the organisation, and that wherever possible and appropriate, records are captured and held in electronic formats’’. (*RMDSR Policy* page 3) Public Health Scotland have a combined *Records Management, Document Storage and Retention Policy (RMDSR Policy)*. The Keeper has been provided with a copy (see element 3). This document includes a combined Business Classification Scheme and Retention Schedule (*BCSRS*). It is based on the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 and the Local Government Classification Scheme (LGCS). It is arranged by function and reference, activity/transaction and retention period. It is ‘‘structured to reflect both the corporate and common types of records held in all parts of PHS.’’ While the format and location of record types is not specifically noted against record classes, the *BCSRS* includes records in various formats including paper, electronic, databases and photographs. Public Health Scotland hold public records in hardcopy and digital format. Digital

	🟨	🟩	records held on various legacy systems, including shared drives (*Retention and Destruction of Electronic Records*, dated 2015, page 1), are currently being migrated to a single electronic document management system, Microsoft 365 (M365). The move to M365 is part of a national project involving all NHS Boards in Scotland, with PHS being one of the pilot authorities. An *O365 Commitment document,* provided as evidence, shows a timeline for implementation including the delivery of staff updates and training as this work progresses. **Work is ongoing to implement the *BCSRS* and the *RMDSR Policy* is in ‘‘iterative development’’. It will be introduced to electronic and paper records as the M365 project continues. The *O365 Commitment document* and the action plan section of the *RMP* for this element note timelines. Updated timelines, following changes to the national M365 pilot project, have been provided separately since submission. These are: SharePoint platform finalised for use December 2021, SharePoint implementation phase December 2021 to December 2022 and benefits realisation in April 2023. Updates on M365 implementation can be provided to the Keeper through the PUR process.** The action plan section for this element notes that PHS are contributing to ‘‘NHS Scotland-wide initiatives on collaborative development of BCSRS and M365’’ and commit to continuing to do so. PHS create and manage records in line of business systems, which will sit outside M365, for example Evadis (*BCSRS* page 15). The Keeper can agree that they are likely to allow the appropriate management of records within a structure as required. PHS have confirmed separately that these systems have been identified by the PHS M365 team and the Information Asset Register (IAR) through the Data Protection

			team and the Digital and Data Review. Offsite storage of physical records is outlined in section 3.1 of the *RMDSR Policy*. A third party storage provider, Oasis Group, deliver this service. A *Process for Archiving Information with RSS* document (RSS are now part of Oasis Group), outlining guidance for staff on to how to send records to long-term storage, has been provided. While the title of this document refers to archiving, it is taken to mean long-term storage for non-current records. The *RMP* (page 11) states ‘‘All paper records are held at Oasis’’. PHS have developed an *Information Asset Register* (IAR) which identifies Information Asset Owners (IAOs) (*Data Protection Policy* - see element 9). An extract of the IAR has been provided. The *BCSRS* will be ‘continually reviewed’’ as it is mapped to both digital and paper records. As the M365 progresses, ‘‘The BCSRS structure will be incorporated into, and implemented with the M365 system and retrospectively applied to existing paper records.’’ The Keeper welcomes these commitments under the action plan section, which includes providing annual updates. (*RMP* page 6) **As a gap in provision has been identified (the application of the *BCSRS* to digital and paper records is ongoing with the roll out of M365) and plans are in place to close this gap (a timeline for this work has been provided), the Keeper can agree this element under ‘improvement model terms’. This agreement is conditional on his being updated on progress.**
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.

	🟨	🟩	Public Health Scotland recognise ‘‘Records management allows us to control the number of records produced through ‘disposal schedules', which explain the time period different types of records should be retained by an organisation.’’ and make the commitment ‘‘that there will be consistent and documented retention and disposal procedures to include provision for permanent preservation of archival records’’. (*RMDSR Policy* pages 2-3) Public Health Scotland have a combined *Records Management, Document Storage and Retention Policy (RMDSR Policy)*. The Keeper has been provided with a copy. (see element 3) This document includes a combined Business Classification Scheme and Retention Schedule (*BCSRS*). The retention schedules are based on the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 (https://www.informationgovernance.scot.nhs.uk/wp-content/uploads/2020/06/SG-HSC-Scotland-Records-Management-Code-of-Practice-2020-v20200602.pdf). **Retention periods ‘‘have either been generated from record types listed in the Scottish Government Records Management Code of Practice or by Corporate Standard.’’ (*RMDSR Policy* page 6). PHS have explained separately that the ‘corporate standard’ is the NHS Scotland Business Classification Scheme. PHS have also explained that ‘‘the policy is currently under review with the aim of creating a unified PHS policy from the 2 legacy appendices, and all aspects of the policy will be reviewed alongside M365 implementation.’’ The Keeper expects to be updated as this work progresses.** While the format and location of record types is not specifically noted against record classes the *BCSRS* includes records in various formats including paper, electronic, databases and photographs. The *BCSRS* is split into two schedules, ‘Document Retention Schedule (Non-

	🟨	🟩	corporate)' and 'Corporate Records Retention Schedule'. These cover health records and administrative records. Retention periods are assigned to each record type, for example: Function and Reference: 32.5 Activity/Transaction: Fixed Term Research and Project Databases Retention Period: Retain for 2 years for quality control purposes following research or project end date. If archiving is not required destroy after the above retention period. If archiving is required, archive for 5 years (if there is a clinical reason to archive longer approval should be sought from Clinical Governance Committee) Identifiers should be removed if archiving Ref: 2.3.4 Activity: Corporate Policy Transaction: Policies Retention: Permanent consider transfer to archive The document control sheet shows that the *RMDSR Policy* underwent staff consultation, indicating local business areas were involved in how retention decisions were allocated. This best practice approach is welcomed by the Keeper as it ensures retention decisions meets the local needs of Public Health Scotland. Any required updates to retention schedules will be agreed by PHS Governance Committees. (*RMDSR Policy* page 6) The *RMDSR Policy* highlights it is the responsibility of all PHS staff to ensure the retention schedule is adhered to and makes clear that allocated retention periods are recommended minimum periods and this should be considered before disposal. As should data protection legislation if considering retaining records containing personal information beyond the stated retention period.

	🟨	🟩	A Corporate Records Management annual review programme is carried out in each directorate or service to monitor adherence to retentions schedules (*RMDSR Policy* page 5). PHS have explained separately that this is an annual review of records reaching their disposition date. It has further been noted that this process will cover all PHS records and will be established following the migration to M365. (see element 13 for further comments on review) Digital**: The *RMP* (page 8) states ‘‘We currently do not have any formal managed electronic records. This risk is accepted by the organisation and a plan to address this is in place. There are therefore no processes for the managed destruction and deletion of electronic information. Implementation of M365 will address both retention and destruction of electronic information on a single platform for PHS.’’ The Keeper can accept the migration to M365 will provide the opportunity to address how allocated retention periods are applied to digital records.** There are processes in place for managing retention and destruction of research records as outlined in the *Research Records Retention Process* document submitted. Line of business: PHS manage public records in line of business systems (systems which will sit outwith M365). The Keeper can agree that records held on these various business systems have specified retention decisions allocated and that these are understood. Physical: The *RMDSR Policy* provides general guidance to staff concerning the application of retention decisions to hardcopy records prior to being sent to offsite storage and the identification of records of ‘‘historical importance’’. The development of guidance for the transfer of records held by the third party storage

			provider for permanent preservation is listed as a planned action. (*RMP* page 10) **The compliance statement for this element notes the *RMDSR Policy* is in ‘‘iterative development alongside the implementation of M365’’. The Keeper expects to be updated on progress.** The action plan section for this element commits to the ongoing development and implementation of retention periods as part of the M365 project and to updating the Keeper annually. This commitment is welcomed by Keeper and indicates recognition that retention schedules will develop and adapt as required by business needs. **The Keeper agrees that Public Health Scotland has schedules providing retention decisions for the record types created while pursuing its functions. However, the authority state that at present electronic records are not able to be formally managed and that this will be addressed through the M365 project. The Keeper can agree this element under ‘improvement model terms’ as a gap in provision has been identified and work is underway to address it. This agreement is conditional on his being updated on progress.**
6. Destruction Arrangements	**A**	**G**	The Act requires that public records are destroyed in a timely, controlled and secure manner. Public Health Scotland acknowledge ‘‘Records management allows us to control the number of records produced through ‘disposal schedules', which explain the time period different types of records should be retained by an organisation.’’ And make the commitment ‘‘that there will be consistent and documented retention and disposal procedures to include provision for permanent preservation of archival records’’. (*RMDSR Policy* pages 2-3)

	🟨	🟩	The following processes are in place for the secure and timely destruction of records: Physical in-house: Secure confidential waste cabinets are available in offices and, after being transferred to secure storage, records are destroyed by a third party contractor, under contract to NHS NSS. A record is kept of confidential waste bags transferred for destruction. The *RMP* also states that when offices are vacated, they are physically inspected to ensure that no records are left behind. 'Disposing of Documents' is addressed in section 5.3 of the *RMDSR Policy*. A document disposal register template is included in this document (appendix B) and records the following details: ''Type of Record, File/Record Name, Format, Brief Description of Record contents, Date Record created, Date Record destroyed, and Method of Destruction''. The records manager is responsible for maintaining this and disposal lists are collected by the records management team. Physical third party storage: Records held offsite with a third party storage provider, Oasis (which acquired RSS), are securely destroyed following their destruction procedures. Several documents relating to these arrangements have been submitted. The *RSS Destruction Process* details the procedures followed by the storage firm to ensure the secure destruction of the appropriate records. These procedures include notifying the customer prior to destruction for review to take place and the provision of destruction certificates. A *Process for Archiving Information with RSS* document, outlining guidance for staff on how to send records to long-term storage, has been provided. This includes information on the application of retention periods and the review of records before destruction. **PHS have confirmed separately that they are currently working on securing a new contract with Oasis after previously being included in a NHS NSS national contract until 2020. The Keeper requests he is notified when this is in place. This can be done through the PUR process.**

	🟨	🟩	<u>Hardware:</u> Secure destruction of hardware with ‘non-volatile memory’ is carried out through NHS NSS , who are PHS’s shared service provider. Several documents have been provided to support this and include, for example, processes for the decommissioning and destruction of CDs, IT equipment and hard drives. PHS also have a *Removable Media Policy,* which forms part of the PHS Information Security Management System (ISMS) (see element 8). <u>Digital:</u> The *RMP* states ‘‘We currently do not have any formal managed electronic records. This risk is accepted by the organisation and a plan to address this is in place. There are therefore no processes for the managed destruction and deletion of electronic information. Implementation of M365 will address both retention and destruction of electronic information on a single platform for PHS.’’ The *Retention and Destruction of Electronic Records* document (this is a NHS Health Scotland document dated 2015) provided also notes this. **The Keeper understands PHS have been in the process of implementing M365 for several years (see element 4). There is a projected completion date for incorporating PHS records into M365 and developing destruction processes for electronic and paper records (*RMP* page 9). The Keeper expects to be updated as these processes are developed and implemented.** PHS have procedures in place for managing the retention and destruction of commissioned research data (physical and digital), ‘‘Unless otherwise agreed, all research data is returned to PHS on completion of the contracted work and disposal managed by PHS directly. Where research data is not retained by PHS, confirmation of destruction is obtained from the researcher.’’ (*RMP* page 19*)* Details of these processes are outlined in the following documents submitted as evidence, *Research Records Destruction (by Commissioned Researcher) Process*, *Research Records Retention Process*, and *Transferred Research Records Destruction Process*. The management of research data is also noted in the document

			Retention and Destruction of Electronic Records. Backups: Recovery and backup restore procedures for NSS systems and servers have been provided (*NSS Commserve Recovery, NSS VMware Recovery Procedure, Comvault backup restore*). The *RMP* explains there is ''backup and replication across servers physically located on different sites.'' And third party IT suppliers provide ''appropriate resilience in their systems to enable disaster recovery.'' (*RMP* page 8) **PHS have confirmed separately that a full list, detailing how long backups are available for before being permanently destroyed, is currently being compiled by PHS IT working alongside NHS NSS as part of NIS audit work. The Keeper can be updated when this list is completed through the PUR process.** The Records Manager (named at element 2) will maintain a destruction log of all records destroyed (*RMDSR policy* page 6). There is an annual Corporate Records Management review programme to ensure compliance with the retention schedule, see element 5. **The Keeper can agree this element of Public Health Scotland's Plan under 'improvement model terms'. This means that he acknowledges that Public Health Scotland have identified a gap in their records management provision (no processes for the managed destruction and deletion of electronic information), but have a long term project underway to address this (see element 4). This agreement is conditional on the Keeper receiving updates as the project progresses. The Keeper also expects to be updated on progress securing a new agreement with an offsite storage provider, and compiling information on the length of time backups are retained.**
7. Archiving and Transfer	**A**	**G**	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. Public Health Scotland acknowledge that ‘‘records are its corporate memory, providing evidence of actions, decisions and representing a vital asset to support its daily functions and operations.’’ (*RMDSR Policy* page 3*)* Public Health Scotland have identified National Records of Scotland (NRS) as the proper repository for the selection of their public records suitable for permanent preservation. 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 **Public Health Scotland have provided a copy of a draft MoU/Transfer Agreement with NRS. Since submission, Public Health Scotland have confirmed the MoU/Transfer Agreement was approved by their Senior Leadership Team and returned to NRS. The MoU/Transfer Agreement is now being processed by NRS. It would be useful if PHS could update the PRSA Assessment Team once this is finalised.** The *RMDSR Policy* section 3.3 addresses the permanent preservation of records. PHS commit to updating the Keeper annually. **The development of guidance for the transfer of records held by the third party storage provider and electronic records for permanent preservation are also listed as actions. The Keeper can be updated on progress on the development of these guidance documents**

	🟨	🟩	**through the PUR process.** **Public Health Scotland have identified a suitable archival repository and a formal MOU/Transfer Agreement with NRS is in the process of being put in place. A commitment to developing guidance around archiving has also been made. The Keeper can agree this element under 'improvement model terms' on the condition he is updated once a formal agreement is in place and as guidance is produced.**
8. Information Security	G	G	The Act requires that public records are held in accordance with information security compliance requirements. Public Health Scotland commit to ensuring ''records will be secure from unauthorised or inadvertent alteration or erasure'' (*RMDSR Policy* page 3) Public Health Scotland have an *Information Security Policy* (version 1.0, dated September 2021) which will be reviewed every two years. The *Policy* (section 4) is clear it covers all records and information held in all formats and applies to ''all PHS staff and contractual third parties with any form of access to PHS information and or information systems.'' It forms part of the PHS Information Security Management System (ISMS) and is part of a suite of twelve PHS Information Security policies developed since submission. The suite also includes a *Clear Desk Policy, Password Policy, Clear Screen Policy, Mobile Device Policy, Third Party Connection Policy and Remote Access Policy*. All these supporting policies were approved in September 2021 or April 2022 and will be reviewed every two years. Copies of all these documents have been provided. The *Information Security Policy* states ''The PHS Board and senior management are committed to preserving the confidentiality, integrity and availability of all information assets throughout the organisation in order to contribute to the health of Scotland by

	🟩	🟩	using data safely and securely ensuring legal, regulatory and contractual compliance.'' The aims of the Policy include ''to support the aims and objectives of the overarching suite of Information Governance Policies, the Information Security Policy Management System (ISMS) and the NHS Scotland Information Security Policy Framework; to facilitate secure information sharing between PHS and other organisations, partnerships and stakeholders; and to ensure compliance with information security and data protection legislation and the common law obligation to preserve the confidentiality of information.'' Staff responsibilities and specific roles, including those of the PHS Board, CE, Senior Information Risk Owner (SIRO), Line Managers and all PHS staff, are outlined in the *Information Security Policy* and supporting policies. The *Information Security Policy* explains that implementation and compliance is monitored by the SIRO and is reported to the Finance, Audit and Risk Committee (*Information Security Policy* pages 6-7). **The *Information Security Policy* states (page 3) ''The PHS suite of Information Governance and Information Security Policies is under development, these will be made available on the PHS intranet and linked to in future versions of this policy.'' The is also a commitment to communicate the *Policy* and associated policies and procedures to all staff (*Information Security Policy* page 4). The *RMP* (page 11) states ''Following approval of the PHS policy, all staff will sign and accept the policy''. The Keeper expects to be updated when this has taken place.** A copy of the *NHS Health Scotland IT Security Policy* (predecessor body, version 3.0, approved 2017) has been provided. NHS Health Scotland and certain areas of NHS NSS became part of Public Health Scotland when it was created in April 2020. The policy sets out the scope, staff responsibilities and measures to ensure records remain secure. These include physical security, password protection, media

	🟩	🟩	disposal, data backup and recovery. It also outlines incident management and reporting measures. The *Policy* notes that all staff must confirm they have read and accept it before being given access to IT systems. **Since submission, PHS have confirmed, following discussions with NHS NSS (who provide most of PHS's IT services) and the development of a suite of PHS Information Security Policies, that a PHS IT Security Policy will be developed by the end of 2022. Updates on the development of this policy can be provided through the PUR mechanism.** A copy of the *NHS NSS Information Security Policy* has been also been provided (version 1.5a, dated 2020, to be reviewed every two years). This covers all types of information in all formats. The above policies explain that PHS have the following procedures in place to ensure the security of its public records: <u>Digital</u>: As noted under element 4, records held on various legacy systems, including shared drives, are currently being migrated to M365. The Keeper is content that information security will be properly considered as M365 is implemented. Access control systems are in place for digital records held on PHS networks, including privilege access management. Password protection and device encryption are in place. Procedures are also in place to ensure security around remote access both for PHS staff and third parties. Recovery and backup restore procedures for NSS systems and servers have been provided (*NSS Commserve Recovery, NSS VMware Recovery Procedure, Comvault backup restore*). <u>Digital line of business</u>: As noted under element 4, Public Health Scotland manage public records in line of business systems (systems which will sit outwith M365). The

	🟩	🟩	Keeper can agree that line of business systems have adequate information security provision as part of their functionality. The *NHS NSS Information Security Policy*) has been provided and addresses the security of NSS data systems. Physical: Records in various formats (e.g. paper, photographs) are referred to in the *PHS Information Security Policy*. Restrictions on physical access are addressed in the *Access Control Policy* (section 5.1) and are controlled and monitored by Information Asset Owners. Information security procedures are in place at the third party storage provider (Oasis) used by PHS (see element 6) which comply with the requirements of ISO 27001 (Compliance | Information Management Services | Oasis Group).The awarding of a contract for third party storage is managed through the *National Contract Statement of Requirement*, which has been provided. Screenshots have been provided showing links to the NHS NSS IT Security Policy and IT Declaration form on the PHS staff intranet site. **As noted above, PHS commit to making the new Information Security Policy and supporting policies available on the same staff intranet site.** PHS use the NHSScotland Security Classification Scheme as outlined in the *Data Classification Policy*. Information risk is managed through risk registers and risk assessments, with an annual Adverse Event Report, which includes information governance, reported to the Public Health and Wellbeing Committee. The *PHS Information Security Policy* (page 6) commits to ensuring ‘‘that all information security adverse events are reported and managed so that lessons learned feed into improvement plans; ensure that where appropriate, adverse events are reported to the appropriate regulatory bodies (e.g. the Information Commissioner’s Office, and/or Scottish Government Cyber Resilience Unit); ensure

			any potential security weaknesses are also reported.'' It also commits to monitoring user access to sensitive data. Guidance on reporting information governance adverse events is available on the staff intranet site. Screenshots showing this have been provided. All staff are required to complete information governance training ('Information Governance in Action') and a screenshot showing access to this training module on the intranet site has been supplied. Additional intermediate training in information governance is available to staff whose responsibilities require it and is mandatory for certain staff. **PHS note several planned actions. These include carrying out penetration testing on network and websites on a regular basis and also monitoring non-compliant mobile devices and software. It is also noted that work will be undertaken to develop staff awareness and training, as well as a training needs analysis for information governance training which will include records management. The Keeper commends these commitments and can be updated on progress through the PUR mechanism.** The Keeper agrees that Public Health Scotland 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. Public Health Scotland is registered as a data controller with the Information Commissioner's Office (ICO): Information Commissioners - Data protection register - entry details (ico.org.uk)

	🟩	🟩	Public Health Scotland have a *Data Protection Policy*. The Keeper has been provided with a copy of this *Policy*. This is version 2.0 dated January 2021. The policy will be reviewed every two years. Public Health Scotland have a Data Protection Officer, Senior Information Risk Officer and Caldicott Guardian. Caldicott Guardians are senior clinical managers of the Board responsible for protecting the confidentiality, privacy and fairness of patients and service-user information and enabling appropriate information-sharing. The *Data Protection Policy* commits to meeting legislative requirements, providing appropriate staff training and outlines the data protection principles which will be adhered to when processing personal data. Staff responsibilities and specific roles are outlined, including Data Protection Officer, Senior Information Risk Owner (SIRO), Caldicott Guardian and Information Asset Owners (IAOs). It also explains that compliance with data protection legislation is monitored through the Finance, Audit and Risk Committee.(*Data Protection Policy* pages 10-13) Data Protection Impact Assessments (DIPAs) will be carried out where necessary and an Information Asset Register (IAR) is maintained. The IAR identifies Information Asset Owners (IAOs) who ‘‘ensure that those information assets which comprise personal data for which they are responsible are managed in compliance with data protection law’’. IAOs are assisted by Information Asset Assistants who ‘‘review the assets regularly on behalf of the IAO’’ (*Data Protection Policy* pages 10-11). All PHS staff are required to report incidents around the processing of personal data and staff responsibilities are outlined on in the *Data Protection Policy* (page 10-13). There is an Adverse Events process for managing data breaches. Staff guidance on

	🟩	🟩	reporting adverse events, including specific information on personal data breaches, is available on the staff intranet. Screenshots showing this have been provided. Staff guidance on data release and data sharing is also available on the staff intranet and screenshots showing this have been provided. Staff are required to undertake mandatory information governance training every two years and a screenshot showing access on the staff intranet site has been provided. Compliance software is to be utilised to monitor staff awareness and agreement to PHS policies including data protection. Copies of *Data Processing Agreement template – CLO Approved, Information Sharing Agreement Template* and *Information Sharing Agreement Instructions* (based on the Scottish Government's Information Sharing Toolkit) have been submitted as evidence**.** A screenshot has been provided showing staff access to these documents on the PHS intranet site. A *Flowchart for approval of work involving personal data* (version 3.1 dated 4 March 2021) has been provided which show the actions to take when dealing with work involving personal data. Where research partners are involved, ''Clear contractual positions are established… to ensure that the Data Controller and Data Processor roles are understood. All data is returned to Public Health Scotland at the end of the project or task for future destruction.'' (*RMP* page 13) The individual identified at element 2 is the PHS Deputy Data Protection Officer. PHS have a privacy notice published on their website at Privacy Notice on Public Health Scotland Website. This includes information about making a Subject Access

			Request (SAR). PHS comply with the Scottish Government Code of Practice for Records Management in Health and Social Care. The Keeper agrees that Public Health Scotland 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. Public Health Scotland has a Business Continuity Management System in place which comprises policies and procedures to ''ensure the ongoing confidentiality, integrity, availability and resilience of records involving personal data.''(*RMP* page 15) PHS have a Business Continuity Plan (version 1.1 Final Draft, dated March 2022), a copy of which has been provided to the Keeper. The *BCP* will undergo a formal review annually and the Business Continuity Team will carry out a testing timetable (*BCP* section 3). PHS have confirmed this *BCP* also covers systems managed by NHS NSS for PHS, and systems managed by 3rd party suppliers (non-NSS). **PHS have confirmed separately that this document has been finalised and approved by the PHS Senior Leadership Team and that appendices are currently being updated. The Keeper can be updated when this work is completed through the PUR mechanism.** **The Keeper has also been provided with a copy of the legacy NHS Health Scotland (PHS predecessor body) *Business Continuity Management Policy* (version 3.0, dated January 2017).** This document provides a framework to allow the authority to resume its functions in the event of an interruption to normal service.

	🟩	🟩	**As noted, this is a legacy policy. PHS have confirmed separately that Business Continuity Policies will be developed. The Keeper can be updated on the development of these policies through the PUR mechanism.** The *RMP* states that vital records are identified and mechanisms are in place to ensure their recovery. The *BCP* (section 1.3) states, ‘‘This Plan is designed to respond to all types of business continuity incidents. A business continuity incident is defined for PHS as; ‘Any event that causes or could lead to the loss of access to processes, people, technology, facilities, and/or vital records required to deliver PHS key business’. It goes on to identify examples of types of incidents, including ‘‘Loss of information (includes cyber attack)’’. PHS have a Business Continuity Team, Business Continuity Lead and Business Continuity Group. The individual named at element 2 is part of the Business Continuity Group (*BCP* Appendix 2). The *RMP* states ‘‘key business data’’ and ‘‘All current information of any importance’’ is held digitally and procedures are in place to manage disruption or loss. The majority of PHS’s IT services are managed by NHS NSS, who also provide HR and Finance services. The *BCP* (section 1.6) states ‘‘At the time of development of this plan discussions to confirm and agree the service levels and support required by PHS from NSS DaS are underway. Once these discussions are complete and service levels and support confirmed this information will be included in this plan.’’ Links are included to relevant NSS business continuity documentation. The *BCP* (section 2.3) includes the roles of the NSS DaS Disaster Recovery Team, NSS/PHS Facilities and Estates and NSS Human Resources, Payroll and Health and Safety during an incident. PHS have confirmed separately that a business continuity table-top exercise is planned for PHS and NHS NSS and will include disaster recovery.

			Recovery and backup restore procedures for NSS systems and servers have been provided (*NSS Commserve Recovery, NSS VMware Recovery Procedure, Comvault backup restore*). The *RMP* states ‘‘An internal audit has been conducted on PHS BC arrangements and deemed them appropriate for the organisation.’’ A copy of this audit, dated January 2021, has been provided. A *Business Continuity Staff Instruction* document (v1.0 dated September 2021) has been provided. It sets out guidance for staff and line managers to follow if normal working is disrupted. Planned actions include Complete Web DR Plan and Test DR plans. The Keeper can be updated on these planned projects as they progress. The Keeper agrees that Public Health Scotland 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	**A**	**G**	The Keeper expects an authority to have processes in place to track public records in such a way that their location is known and changes recorded. Public Health Scotland will ensure ‘‘that access and disclosure will be properly controlled and audit trails will track all use and changes’’. (*RMDSR Policy* page 3*)* **Public Health Scotland state formal audit trails are not in place for unstructured information. This is also made clear in the *NHS Health Scotland Retention and Destruction of Electronic Records* document, which also notes there is no consistent naming convention.**

	🟨	🟩	Public Health Scotland acknowledge the importance of version control in making information (policies and procedures, guidelines and newsletters) available to staff via the intranet site, ‘‘There must be a single definitive version of every document made available on the intranet, and where required, automated documents links will be used to cross-refer to the document from other intranet sites and documents. This will ensure that a single version of the document exists.’’ (*RMDSR Policy* page 4) **The migration of records from ‘‘legacy platforms’’ to M365 is underway and SharePoint will provide automated version control. Public Health Scotland intend to introduce formal version control and naming convention processes and guidance as part of the M365 implementation. The action plan section under this element notes that the introduction of M365 ‘‘will enable an audit trail of both electronic and paper records.’’ The Keeper would like to be informed when these processes and guidance are in place and operational.** Public Health Scotland do not consider it necessary to have manual tracking controls in place for paper records as the volume of this material is small and decreasing. Paper records are held in third party storage and are subject to access and location tracking with the specified requirements outlined in the *RSS Contract* and explained in the *RSS destruction process*. The use of destruction logs is also in place. **Public Health Scotland have identified a gap in provision (formal audit trails are not in place for unstructured information and there is no consistent naming convention in operation) and are working to address this, for both paper and digital records, with the implementation of M365 and development of appropriate guidance. As such, the Keeper can agree this element under ‘improvement model terms’ and expects to be updated on progress.**

	🟨	🟩	
12. Competency Framework for records management staff	**G**	**G**	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported. Public Health Scotland have committed to ensuring ‘‘all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance’’ and that ‘‘Specific Records Management training will be developed alongside other PHS staff training currently in development.’’ (*RMDSR Policy* page 5) PHS state they have in place ‘‘CPD/PDP arrangements for all staff, including its information and records professionals, and allocates resources for their training. Internal records management training will be developed for all PHS staff as M365 is deployed.’’ (*RMP* page 17) Information Governance and Freedom of Information training is mandatory for all PHS staff and must be taken every two years. Additional intermediate training from an external body is required for specific staff, including those with information governance responsibilities and is recommend for senior managers. A screenshot of the PHS intranet site showing access to the training module (‘Information Governance in Action’) and additional training from an external provider has been submitted. Staff completion details are recorded on the training platform. Completion of training is included in the PHS *staff induction checklist*, a copy of which has also been provided. PHS utilise the *NHS Scotland Information Governance Competency Framework*, a copy of which has been provided. This document also informs continuous and professional development for staff with information governance and records management responsibilities. An extract of the *Objectives and PDP for SPRDDPO* (named at element 2) has been provided. Training achieved by the post holder is

			noted at element 2. **The development of a records management training module which will include M365 is noted as a planned action. The development of a training needs analysis for information governance which will include records management is also noted as an action (*RMP* page 12). Other planned actions noted include developing training and instructions around transfer of records to archival storage (*RMP* page 10), information security (*RMP* page 11), and version control and file naming (*RMP* page 16). The Keeper would like to be kept informed as these resources are developed.** The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, he agrees that Public Health Scotland consider information governance training for 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. Public Health Scotland commit to ensuring ‘‘that the application of records management procedures is regularly monitored against agreed standards and action taken to improve standards as necessary’’. (*RMDSR Policy* page 3) The *CEO letter* makes the following commitment ‘‘As a young organisation which is building on the legacies of organisations from across NHS Scotland, we are committed to ongoing development of our records management approach, bringing together knowledge and experience from those organisations and consolidating this within the Public Health Scotland plan.’’ Public Health Scotland will review their records management arrangements annually through corporate reporting and engaging with the NRS PUR process. An annual

	🟩	🟩	review of arrangements will form part of an annual information governance report to the PHS Public Health and Wellbeing Committee. An annual Corporate Records Management review programme ‘‘reviews each directorate or service area’s compliance with this policy…’’ (*RMDSR Policy* page 5). PHS have explained separately that this review will ‘‘be presented to the Information Governance Board, with elements of that incorporated into the annual report on information governance presented to the Public Health and Wellbeing Committee.’’ PHS have confirmed that routine reporting on ‘‘the action plan generated from the RMP’’ to the Information Governance Board will take place (see element 2 and general comments below on IG Board). It has further been explained separately that the migration to M365 will assist in reporting on records management, along with reviews of the IAR and off-site storage. In addition, systems which will sit outside M365 have been identified as part of this project and that once M365 implementation is completed a further review of PHS records will be carried out by each Directorate. The Keeper commends these plans to carry out additional reviews. Internal audit will be used to review records management. Information governance, including records management is part of an annual audit cycle. PHS have confirmed separately that the 2020-21 internal audit plan was approved by the Finance, Audit and Risk Committee. A copy of *PHS Data Governance Audit report* (dated June 2021) has been provided. This was carried out by an external auditor and includes records management as one of the key areas of focus. PHS have confirmed separately that the Senior Policy, Risk and Deputy Data Protection Officer, named at element 2 is responsible for reviewing the RMP and its implementation.

			The Keeper commends the commitment to provide annual updates on reviews through the PUR reporting mechanism. Both the *Data Protection Policy* and *Records Management, Document Storage and Retention Policy* are to be reviewed every two years, with respective review dates of March 2022 and June 2023. PHS have a policy tracker to ensure reviews are carried out as scheduled. The *Records Management, Document Storage and Retention Policy* has been added to the tracker. In addition, the *Information Security Policy* and supporting policies are to be reviewed every two years. The *Business Continuity Plan* will undergo a formal review annually and the Business Continuity Team will carry out a testing timetable (see element 10). The Keeper agrees that Public Health Scotland 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. Furthermore he agrees that supporting policy and guidance documents have appropriate review periods allocated.
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. Public Health Scotland is a ‘‘data driven organisation that receives personal data from a range of sources’’. (*RMP* page 19) PHS control and manage the sharing of data with other NHS Boards under the Intra NHS Data Sharing Accord (not submitted but available online, Intra-NHS Scotland Information Sharing Accord (2020) | Information Governance) and other third parties through the use of Information Sharing Agreements based on the Scottish Government Information Sharing Toolkit.

	🟩	🟩	Section 7 of the *Information Security Policy* addresses information sharing. A *Third Party Connection Policy* specifically addresses information security and governance processes for contracts and agreements between PHS and third party suppliers. Copies of an *Information Sharing Agreement Template* and *Information Sharing Agreement Instructions* have been submitted as evidence**.** PHS has provided a *NHSS Standard Contract Template* which includes provisions for maintaining confidentiality of any information used by the contractor and also a requirement to comply with data protection legislation. Also submitted is a *Research Services Contract Agreement Template* which sets out the arrangements for research projects using personal data. Again, it includes provisions for maintaining confidentiality of any information used by the contractor and also a requirement to comply with the data protection legislation. It is also noted that ‘‘all research data is returned to PHS on completion of the contracted work and disposal managed by PHS directly. Where research data is not retained by PHS, confirmation of destruction is obtained from the researcher.’’ (*RMP* page 19) The *Research Records Retention Process* outlines the steps taken for providing controlled and secure access to and sharing of research records and compliance with data protection legislation. *Scottish Government Circular CEL25/2011* has also been submitted. It provides guidance for safeguarding personal data which may be used by third-party contractors. **The action plan section notes all data sharing and processing agreements are to be reviewed and updated and a record of each document to be included in the IAR. The Keeper can be updated as this work progress through the PUR**

	🟩	🟩	**mechanism.** The PHS Privacy notice Organisational background - Our privacy notice - Public Health Scotland and Model Publication Scheme Public Health Scotland model publication scheme - Publications - Public Health Scotland, both published on the PHS website, outline how to access information and the model publication scheme explains the type of information that is routinely published and how to access it. (*RMP* page 10) The Keeper can agree that Public Health Scotland properly considers records governance when undertaking information sharing programmes.
15. Public records created or held by third parties	**N/A**	**N/A**	The Public Records (Scotland) Act 2011 (PRSA) makes it clear that records created by third parties when carrying out the functions of a scheduled authority should be considered 'public records' - PRSA Part 1 3 (1)(b). Public Health Scotland have confirmed it does not contract out any of its functions to a third party. The *RMP* (page 20) states ''PHS has not tasked any third parties to carry out its functions. While PHS makes use of contractors and suppliers to help deliver services, these third parties operate to the direction and instruction of PHS. All public records created as part of this service delivery are held by PHS.'' The Keeper agrees that Element 15 does not apply to Public Health Scotland.

General Notes on Submission:

Version

This assessment is on the Public Health Scotland Records Management Plan (the *RMP*) originally submitted to the Keeper for his agreement on 12th July 2021, updated, approved and resubmitted on 26 May 2022. This is version 1.0 and is dated 19 May 2022. It is signed by Scott Heald, Director of Data and Digital Innovation, Public Health Scotland (see element 1). The control sheet notes it will be reviewed in May 2023.

The *CEO letter* makes the following commitment ''As a young organisation which is building on the legacies of organisations from across NHS Scotland, we are committed to ongoing development of our records management approach, bringing together knowledge and experience from those organisations and consolidating this within the Public Health Scotland plan.''

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

The introduction of the *Records Management, Document Storage and Retention Policy* acknowledges ''PHS records are its corporate memory, providing evidence of actions, decisions and representing a vital asset to support its daily functions and operations. They support policy formation and managerial decision-making, protect the interests of PHS and the rights of health professionals, trainees, staff and members of the public who have dealings with PHS. They support continuity, accountability, efficiency and productivity and help deliver its services in consistent and equitable ways.''

Key Group

PHS have confirmed that an Information Governance Board has been established and the first meeting took place on 30th March 2022. The Board's remit includes records management. The Board reports to the Senior Leadership Team and the Public Health and Wellbeing Committee.

Local Records Management

Information Asset Owners (IAOs) are in place at Public Health Scotland and are identified in the Information Asset Register (IAR). They are supported in their role by Information Asset Assistants.

IAO’s are responsible for carrying out ‘‘the required information risk assessments (data protection information assessment (DPIA) and system security plan (SSP)) for all IT and data services when: significant changes are proposed to an existing service; prior to implementation of new IT and information systems; a significant information security adverse event has occurred.’’ (*Information Security Policy* page 5)

IAO’s control and monitor physical access to information assets (Access Control Policy page 5) and ‘‘are responsible for ensuring that information risk assessments (data protection impact and system security policy assessments) are carried out, that the information is classified appropriately and that the relevant security measures (both electronic and physical) are in place and that a register of information assets, for which they are responsible, is maintained.’’ (*Data Classification Policy* section 8.3*)*

IAOs ‘‘ensure that those information assets which comprise personal data for which they are responsible are managed in compliance with data protection law’’ and Information Asset Assistants ‘‘review the assets regularly on behalf of the IAO’’ (*Data Protection Policy* pages 10-11).

Further IAO responsibilities are outlined in the *Encryption Policy, Password Policy,* and *Third Party Connection Policy.*

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 ***Public Health Scotland.*** Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development by ***Public Health Scotland*** are as follows:

Element 4 Business Classification
Element 5 Retention Schedule
Element 6 Destruction Arrangements
Element 7 Archiving and Transfer
Element 11 Audit Trail

7. Keeper’s Determination

Based on the assessment process detailed above, the Keeper agrees the RMP of ***Public Health Scotland***

- The Keeper recommends that *Public Health 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,

E. Course

Liz Course
Public Records Officer

Pete Wadley
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 ***Public Health Scotland*****.** In agreeing this RMP, the Keeper expects *Public Health Scotland* to fully implement the agreed RMP and meet its obligations under the Act.

……………………………………………

Paul Lowe
Keeper of the Records of Scotland