Public Records (Scotland) Act 2011

Scottish Information Commissioner

The Keeper of the Records of Scotland

28th July 2023

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 Information Commissioner by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 30th June 2021.

The assessment considered whether the RMP of the Scottish Information Commissioner 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 Information Commissioner complies with the Act can be found under section 7 of this report with relevant recommendations.

2. Authority Background

The Scottish Information Commissioner is a public official appointed by Her Majesty the Queen on the nomination of the Scottish Parliament. The Commissioner is responsible for enforcing and promoting Scotland's freedom of information laws, namely:

The Freedom of Information (Scotland) Act 2002
The Environmental Information (Scotland) Regulations 2004
The INSPIRE (Scotland) Regulations 2009

The Scottish Information Commissioner investigates applications and issues legally enforceable decisions; promotes good practice amongst public authorities; and provides the public with information on their rights.

Homepage | Scottish Information Commissioner (itspublicknowledge.info)

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 Information Commissioner'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. The submitted records management plan (*RMP*) of the Scottish Information Commissioner (SIC) identifies Daren Fitzhenry, the Scottish Information Commissioner, as the individual with overall corporate responsibility for records management. The *RMP* includes a signed *Covering Statement* from Mr Fitzhenry (dated 30 June 2021) which makes the following commitments: • "our policies, procedures and practices are implemented and that they are effective • we routinely review and develop as necessary our policies, procedures and practices • all staff maintain, and develop as necessary, their competence in information and records management • all employees, contractors, agents, consultants and other third parties who have access to any information held within the Commissioner's office, are fully aware of and abide by their information and records management duties under the PRSA." This identification is supported by section 3 of the *Information and Records Management Policy*, which outlines roles and responsibilities.

			Reports are regularly provided to the Commissioner on information and records management as outlined in *Governance Reporting Arrangements*, a link to which has been provided. The Keeper agrees that the Scottish Information Commissioner 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 SIC have identified, Helen Gardner-Swift, Head of Corporate Services, as the individual holding operational responsibility for records management. This identification is confirmed in the Commissioner's *Covering Statement* and is further supported by section 3 of the *Information and Records Management Policy*, which outlines roles and responsibilities. Section 9 of the *Information and Records Management Handbook* includes a competency framework for the role of Head of Corporate Services. It lists the information and records management responsibilities of the post and the required core skills and attainment method. The Head of Corporate Services is the responsible manager for key policies and procedures including the *Information and Records Management Policy*, *Information and Records Management Handbook*, *Employee handbook, Business Continuity Policy*, *Data Protection Policy and Handbook,* and *File Plan and Retention Schedule*. The post-holder is also the approver of *Records Review Procedures*.

			The Head of Corporate Services is a member of the Data Protection Officer (DPO) Networking Group and meets with the DPO annually. She also chairs the GDPR Working Group (see element 9). The post holder also has lead responsibility for business continuity planning implementation (see element 10). The *Governance Reporting Arrangements* document further supports this and confirms the identification of the Head of Corporate Services as designated manager responsible for routine reporting to the Senior Management Team (SMT) or Commissioner on information and records management. The *Information and Records Management Handbook* (section 10) and *Data Protection Policy and Handbook* (page 15) detail the responsibilities of the Head of Corporate Services around compliance monitoring (see elements 9 and 13). The Keeper agrees that the Scottish Information Commissioner 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 SIC have an *Information and Records Management Policy*. A link to which has been provided to the Keeper. This is version 02.05 approved 30 June 2021 and updated December 2022 to reflect planned review date of July 2023. The *Policy* will be reviewed annually. The *Policy* is published online on the authority's website, InformationandRecordsManagementPolicy.pdf (itspublicknowledge.info). The *Policy* states, "The Scottish Information Commissioner (the Commissioner) recognises the value of our records as a corporate asset and records management as a key corporate function. Our records provide evidence of actions and decisions

			and support our strategic objectives and operational functions. Having effective records management arrangements also helps us to: • increase efficiency and effectiveness, delivering savings in administration costs • improve and develop service delivery • achieve business objectives and targets • ensure compliance with the Public Records (Scotland) Act 2011 and other legislative requirements, standards and codes of conduct • support transparency and open government • underpin business resilience" The *Policy* applies to all SIC staff and relates to records in all formats. It includes a policy statement; and sections covering review, retention and disposal arrangements; roles and responsibilities; performance review and compliance monitoring; relevant legislation and regulations; and information security. The *Information and Records Management Policy* is supported by suite of guidance and procedural documents, including the *Information and Records Management Handbook* (version 04.02 approved 30 June 2021), *File Plan and Retention Schedule* (version 02.13 last updated 19 Feb 2019), and *Records Review Procedures* (version 02.18 last updated 12 Dec 2022). All which are published on the authority's website and links have been provided. Staff are required to confirm they have read and understood the *Information and Records Management Policy* and *Handbook* annually (section 1, *Handbook*). As noted above, the *Policy* is also published online. The Keeper can therefore agree SIC staff are able to access it. The *RMP* outlines actions under the future developments section relating to changed working arrangements as a result of the impact of Covid-19 and the provision of staff guidance to reflect this. The Keeper welcomes these assurances on the information governance measures that were put in place. A commitment is given to reflecting any such changes in future updates to the *Policy*. It has been

			confirmed separately that the SIC office premises re-opened in May 2022 and the authority are now in a trial period of hybrid working. The Keeper agrees that the Scottish Information Commissioner have 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 SIC have a function-based file plan (business classification scheme) which forms part of the combined *File Plan and Retention Schedule* (version 02.13 dated March 2019). A link to this document, which is published on the authority's website, has been provided. The *File Plan* is arranged by function, activity and sub-activity. The *RMP* states it "provides a framework for a consistent approach to classifying all records across the organisation regardless of format or records storage location.." And "the File Plan, in conjunction with the Retention Schedule, is used to identify and retrieve records relating to the same function and activity anywhere in the organisation, irrespective of which department produces or receives them." Paragraph 14 of the *Information and Records Management Handbook* notes, "Our records must be trustworthy, complete, accessible, legally admissible in court, and robust for as long as our File Plan and Retention Schedule requires. Records that are consistently created, stored correctly and logically indexed are easier to manage to meet these requirements." The SIC operate a hybrid recordkeeping system with digital and hardcopy records. Digital records are managed in several software systems and network drives.

			The *Information and Records Management Handbook* outlines the systems in use and details procedures and staff guidance on use: Digital EDRMS – Virtual Cabinet (VC) is noted in the extract from the *Risk Register*, provided to the Keeper, as being the EDRMS. It used for corporate records, including HR records. Line-of business systems – Workpro, which uses Workday, is used to manage case records. Digital shared network and PC drives - The *Information and Records Management Handbook* (para 58) notes "Exceptionally, there may be justification for holding records in a network drive. The following section describes when it is appropriate to do so." Records stores on network drives are which are managed in line with the file plan. A screenshot of the P:Drive showing this is included in the *Information and Records Management Handbook* (paragraph 62). This includes systems such as Sage, for financial records. MS Outlook is used for emails. Guidance on identifying which emails are records and saving them to the appropriate system is detailed in section 5 of the *Information and Records Management Handbook.* At the time of submission MS Teams was in use for online meetings. The management of additional functionality, such as recording and chat, is outlined in the *Information and Records Management Handbook.* Hardcopy (paper and memory sticks) records are managed onsite in locked areas and in a secure store. Hardcopy public records are listed in a register on the relevant digital system. It has been confirmed separately that "The management of paper records has been updated following the move to remote working and

			hybrid working. As far as possible, paper records are not created or held and all new records should be held electronically and managed via our records management systems using VC and WorkPro." Additional guidance was issued to staff with move to remote working in 2020. An extract from this guidance has been provided. The *Information and Records Management Handbook* provides procedures and staff guidance on the use of records management systems, which system to store records in (digital and paper) and how to create appropriate metadata by indexing. Guidance specific to the Workpro system is contained in the *Investigations Handbook* (paragraphs 166-167 and appendix 7). This document is published on the on the authority's website. The *File Plan and Retention Schedule* includes guidance for staff. Part 3 of the document provides guidance on maintenance and review, including how annual reviews are carried out and amendments made. The Head of Corporate Services is responsible for ensuring reviews are carried out and outcomes reported to senior management. **The *RMP*, under the future developments section, notes that at the time of submission the *File Plan and Retention Schedule* was undergoing a review and being updated. This action was part of the authority's Operational Plan 2021-22. It has been confirmed separately that the review of the File Plan and Retention Schedule project is continuing into 2023-4. This follows a recent upgrade of VC. SIC have committed to providing an update to the Keeper when approved. The Progress Update Review (PUR) mechanism can be used for this.** The Keeper agrees that the Scottish Information Commissioner 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	**G**	**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 Scottish Information Commissioner has a combined *File Plan and Retention Schedule*. A link to this document, which is published on the authority's website, has been provided. The *Retention Schedule* includes records in all formats and locations. The *RMP* states, ''The Retention Schedule ensures that the same types of records should be managed consistently no matter where the record is held, or who created it.'' And ''The retention periods are determined by legal, statutory and business requirements.'' The following is an example entry from the Retention Schedule: Activity / Records Series - Quotes and related correspondence Examples of Record Types - Evaluations of application from prospective suppliers: Successful Trigger - End of contract Retention Period – 5 years Action - Destroy Custodian - HOCS Authority - Statutory Citation/Notes - Legislation Location – VC, paper The *File Plan and Retention Schedule* provides staff guidance including information

			about the destruction of records, and use of destruction registers (see element 6). Part 3 of the document provides guidance on maintenance and review, including how annual reviews are carried out and amendments made. The Head of Corporate Services is responsible for ensuring reviews are carried out and outcomes reported to senior management. The *Information and Records Management Handbook* outlines procedures and staff guidance on how records (digital and paper) within each of the systems in use are managed throughout the records lifecycle. For example, paragraph 38 states "Throughout the lifecycle of a record you must ensure that the metadata relating to the record remains current and appropriate and that the record is filed and managed in accordance with the File Plan and Retention Schedule". Section 7 of the *Handbook* details the records review procedure and notes "a review of all records held should be carried out on an annual basis for each function." This is carried out by Heads of Departments, following the *Records Review Procedure*. The *Records Review Procedure*, which is published on the authority's website, provides guidance on the implementation of the *File Plan and Retention Schedule*. It details records review procedure for all records systems in use by SIC. This is also outlined in the section 2 of the *Records Management Policy*, which explains "The Finance and Administration Manager (FAM) (assisted as required by a member of the Corporate Services Team (CST)) will meet annually with each Head of Department to discuss the functional file plan and the associated records retention schedule to ensure that they remain current, and are amended as appropriate to reflect any changes to the information held e.g. following the commencement of any new activity." The *Records Review Procedure* (paragraphs 31-32) explains how the Head of Corporate Services oversees the stages of the review procedure including

			authorisation for the destruction of records. This involves a first and second review process with the second reviewer verifying the action taken by the first. This is done for both digital and paper records. This is followed by notification to the Head of Corporate Services who gives final authorisation before records are deleted. The Head of Corporate Services will action any changes to the Retention Schedule as a result of the review process (paragraph 38). The *Records Review Procedure* includes a template 'File Plan and Retention Schedule Amendment Form' (appendix 2) and 'VC Feedback Form' (appendix 3). The process of identifying records which have reached their retention period and are due for review is manual for Virtual Cabinet (VC) and network drives. Identification of records due for review is an automated process in the Workpro system. This will be carried out by the Corporate Services Team or individuals where access to file management functions is restricted certain systems. Paper records are identified for review by the Corporate Service Team. The possible actions at the point of review are listed in the *Records Review Procedure* as destroy, reviewed (records reviewed and decision taken to retain), retain – KM (determined that there is value in further retention for a short term for knowledge management value and to subsequently be reviewed annually), and permanent archive (records to be permanently retained outwith retention schedule). The Retention Schedule indicates some record types which may be considered for transfer to National Records of Scotland (NRS). See element 7 for archiving. The future developments section notes the delay to a planned project to revise retention periods with the intention of creating "more automated processes and tasks to support the records review processes subject to our duties and responsibilities as regards data protection and personal information." At the time of submission, the *Records Review Procedures* and *File Plan and Retention Schedule* were under review. As noted above this work will continue into 2023-24. A

			commitment is made to providing the Keeper with updated approved versions. The Keeper agrees that the Scottish Information Commissioner has a schedule providing retention decisions for the record types created while pursuing its functions.
6. Destruction Arrangements	**G**	**G**	The Act requires that public records are destroyed in a timely, controlled and secure manner. The *Records Management Policy* (paragraph 18) states "The Commissioner has suitable arrangements in place for the destruction of records, in accordance with the Retention Schedule. Records of destruction are created and retained in accordance with the Retention Schedule. Provision is made for the secure destruction of paper waste, including confidential paper waste and the assured secure destruction of sensitive digital records. The arrangements also cover the assured secure destruction of hardware and back-up media used to store digital records." The *File Plan and Retention Schedule* (paragraph 84) notes, "Disposal of records is an important part of records management and ensures that the organisation retains records only for as long as they are needed and then disposes of them in an appropriate manner." The *File Plan and Retention Schedule, Records Review Procedure* and *Information and Records Management Handbook*, all of which are published on the authority's website, outline procedures in place for the destruction of digital records in each of the systems in use by the SIC. This includes the recording of any destruction undertaken in a destruction register. The *Records Review Procedure* (paragraphs 31-32) provides detailed staff

			guidance, including screenshots and flowcharts, and explains how the Head of Corporate Services oversees the stages of this procedure including authorisation for the destruction of records (see element 5). The destruction of paper records is explained in *Records Review Procedure* and *Information and Records Management Handbook.* Paper records selected for destruction after being reviewed are shredded after being placed in secure locked consoles. A contract is place with an external company for the secure destruction of waste paper from these consoles. A copy of a sample destruction certificate has been supplied. The permanent destruction of emails, including back-ups is explained the *Information and Records Management Handbook* (section 5). The disposal of IT hardware is addressed in section 8 of the *Information and Records Management Handbook.* The Head of Corporate Services (named at element 2) authorises such disposals. Destruction is carried out by a third-party provider and a destruction certificate is provided. A copy of a sample certificate of destruction has been provided. The *Information and Records Management Handbook* notes daily back-ups being taken from network drives. A statement has been provided separately confirming arrangements in place for the destruction of back-ups, explaining the frequency and time scales for retention of encrypted back-ups. The *File Plan and Retention Schedule* (paragraphs 19-22) explains that two destruction registers are used by the SIC. Both are in the form of a spreadsheet and are saved in VC with access controls in place. One is used to record the destruction of organisational records and one for the destruction of confidential HR records. A full list of the information to be captured in the register is given in paragraph 128 of

			the *Records Review Procedure*. Extracts from destruction registers showing records destroyed in VC and the destruction paper records have been supplied. Destruction registers and disposal certificates are allocated a permanent retention period in the retention schedule (page 46). The future developments sections notes the delay to a planned project to revise retention periods with the intention of creating "more automated processes and tasks to support the records review processes subject to our duties and responsibilities as regards data protection and personal information." At the time of submission, the *Records Review Procedures* and *File Plan and Retention Schedule* were under review. As noted above, work is ongoing, and a commitment is made to providing the Keeper with updated approved versions. The Keeper agrees that the Scottish Information Commissioner has processes in place to irretrievably destroy their records when appropriate.
7. Archiving and Transfer	**G**	**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. The SIC have identified National Records of Scotland (NRS) as the proper repository for public records suitable for permanent preservation. NRS is an accredited archive, NRS' Archive Service Accreditation Success | National Records of Scotland (nrscotland.gov.uk) and fully adheres to the Keeper's Supplementary Guidance on Proper Arrangements for Archiving Public Records. The SIC have a formal agreement in place with NRS that governs the transfer of

			records. However, the Memorandum of Understanding (MoU) under which these arrangements operate was signed in 2014 and is now out-of-date and an updated agreement is required. This is acknowledged in the *RMP* which notes that a revised MoU/deposit agreement is being discussed. The *RMP* also notes, "The MOU identified records which we may wish to transfer in the future. However, there are no immediate plans to transfer as yet, as those records we have identified may still be of operational benefit to us." It has been confirmed separately that this matter will be pursued, and a meeting arranged to further discuss updating the agreement with NRS. It has also been confirmed that once an updated agreement is in place the Keeper's assessment team will be notified. The PUR mechanism can be used to provide updates. The *RMP* commits to fulfilling the requirements of the NRS Deposit Agreement for Electronic Records. The *RMP*, under the future developments section, notes that procuring a new website was part of the authority's Operational Plan 2021-22, with work expected to span 2021-24. It has been confirmed separately that a new website was put in place in 2021-22 and went live at the start of 2022-23. Archiving and transfer arrangements were considered and taken account of in the specification and design of the new website. The SIC worked with NRS when developing the new website and it is part of the NRS web archive. The Keeper agrees that the Scottish Information Commissioner has arrangements in place to properly archive records when appropriate.
8. Information Security	**G**	**G**	The Act requires that public records are held in accordance with information security compliance requirements.

			The *RMP* states that the Commissioner "recognises that information is a valuable asset and that business continuity is dependent on its integrity and continued availability." And is "…committed to the secure use of information and information technology systems in order to protect the availability, integrity and confidentiality of the information under our control." These commitments are echoed in the information security policy statement which forms part of the *Information and Records Management Policy* (section 6). The *Policy* states "Each member of staff must follow the procedures and controls within the Information and Records Management Handbook and the Principles on the Use of the Internet and Email (Part 2, Section 5 Professional Conduct of the Employee Handbook), and any other associated guidance which has been issued relating to the management of systems and the information contained on those systems." In order to monitor risk and resilience, a risk register is maintained. An extract has been supplied showing provision for information security. It outlines risks, controls in place and actions planned. This extract includes measures in place for digital records and physical information security. The introduction of the *Information and Records Management Handbook* states "The Commissioner provides the necessary software and drives for storing information which have the appropriate access permissions, security and are backed-up." Back-up arrangements have been explained separately (see element 6). Information security procedures and staff guidance are detailed in the published *Information and Records Management Handbook*. These include the secure use of software systems (section 4), email and other systems including MS Teams. Role specific access restrictions are place for certain systems and drives, and password protection is in place. Procedures and guidance are in place for hardware (including

			PCs, laptops, encrypted memory sticks and mobile phones) (section 3). Physical security procedures and guidance are in place for the storage of records, both digital and hardcopy (paper and memory sticks) (section 6). Paper records are stored in locked areas and managed through a paper record register (see element 11). As noted at element 6, the SIC undertake the destruction of records and IT hardware in a secure manner. The *Information and Records Management Handbook* is supported by the *Data Protection Policy and Handbook* and *Employee Handbook*, both of which are published on the authority's website. SIC have a security vetting policy and procedures which are outlined in the *Employee Handbook* (paragraphs 517-528). The *Data Protection Policy and Handbook* (paragraphs 72-89 and appendix 6) addresses information security and the reporting of security and data breaches. The Keeper has also been provided with extracts of a clear desk policy and additional staff guidance on remote working which includes maintaining the security of information and who to contact in the event of a data incident or breach. The *Investigations Handbook* (appendix 7) also contains records management guidance on the security of hardcopy casefiles/information. This document contains procedures and staff guidance for undertaking the investigations process. The SIC have achieved Cyber Essentials and Cyber Essentials Plus accreditation and commit to ensuring this is maintained. Copies of accreditation certificates have been provided. The authority also follows Scottish Government guidance on cyber security and participates in the Public Sector Action Plan as part of the Cyber Resilience Strategy issued by the Scottish Government. Cyber security is addressed in the *Information and Records Handbook* and *Data Protection Policy and Handbook*. The Keeper commends this thorough approach to cyber security resilience.

			The Keeper acknowledges and commends the noted security measure reviews carried out by the authority in 2015-16 and 2017-19, and the resulting improvements. The *RMP* commits to regularly reviewing information security measures. The Head of Corporate Services (named at element 2) will undertake a review of compliance with security arrangements (IT and paper) in the *Information and Records Management Handbook* every three years (*IRM Handbook* section 10). As noted at element 4, the Keeper welcomes the information provided around measures put in place noted under future developments following changes to working practices as a result the Covid-19 pandemic. The Keeper agrees that the Scottish Information Commissioner 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. Since the Keeper last agreed the *RMP* of the Scottish Information Commissioner in 2014, new data protection legislation has come into force. The *RMP* explains the measures the Scottish Information Commissioner has put in place following an implementation project led by the Head of Corporate Services (named at element 2) and assisted by the GDPR Working Party. The SIC updated and revised their *Data Protection Policy and Handbook* (v02.07, approved March 2021) to reflect this. The *Handbook* is published on the authority's website. This document outlines procedures in place and staff guidance. The *RMP*

			notes that staff were made aware of updates and how to access the updated document. This document was due to be reviewed in March 2023. The *Data Protection Policy and Handbook* states "The SIC aims to ensure that all personal data is processed in a way that is lawful and correct in accordance with the DPA 2018 and the UK GDPR principles however it is collected, recorded and used, irrespective of its format and including for example paper copies, computer records, datasets and data held on applications and devices." The *Policy* explains the data protection principles and data protection by design and default. The SIC are a registered data controller (ICO registration reference Z8091699). A Data Protection Officer (DPO) is in place. The *RMP* explains that the Scottish Parliamentary Corporate Body (SPCB) provides a shared DPO service. An MOU is in place to govern this arrangement and renewed annually. The future developments section of the *RMP* notes that the MOU with SPCB has been reviewed, but at the time of submission the signing had been delayed due to the impact of the Covid-19 pandemic. It has been confirmed separately that the updated MOU was signed by the Commissioner on 24 September 2021 and is operational The appointed DPO is Robin Davidson. An alternate DPO is also in place in the event of a conflict of interest. Contact details are provided in the *Data Protection Policy and Handbook.* The *RMP* explains how the Head of Corporate Services (named at element 2) and the authority's Senior Management Team (SMT) liaise with the DPO through annual meetings and membership of a DPO Networking Group. This is supported by the *Data Protection Policy and Handbook* (paragraphs 94-106) which outlines governance arrangements and the compliance monitoring responsibilities of the

			Head of Corporate Services. This includes a quarterly report to the SMT and providing assurance the *Data Protection Policy and Handbook* is being adhered to. Procedures and staff guidance are in place for recording and managing data breach incidents. These, and information security measures are outlined in the *Data Protection Policy and Handbook* (paragraphs 72-89 and appendix 6). Information security procedures and guidance are detailed in the *Information and Records Management Handbook.* The SIC use Data Protection Impact Assessments (DPIAs) where required. The processes in place and staff guidance on DPIAs are detailed in the *Data Protection Policy and Handbook* (paragraphs 61-66 and appendix 5). The *RMP* explains the SIC revised contracting guidance and model terms and conditions, and updated Committee Report templates to reflect changes to data protection legislation in 2018. The *Data Protections Policy and Handbook* outlines procedures in place for contracts (paragraphs 39-42). The SIC have a Privacy Notice published on their website, Privacy notice | Scottish Information Commissioner (itspublicknowledge.info). It provides information on how to contact the authority to exercise data protection rights. The *RMP* notes the Privacy Notice is designated a key document and regularly reviewed. Subject Access Request (SAR) procedures and staff guidance are detailed in appendix 3 of the *Data Protection Policy and Handbook* and in *Responding to Information Requests: Guidance and Procedures*, which is also published on the authority's website. The SIC *Employee Handbook* contains a specific section on data protection (paragraphs 488-516) and outlines staff responsibilities, including when working

			remotely. Data protection responsibilities for staff when remote working are also addressed in extracts from *Additional Temporary Guidance Remote Working (records management (Managing Information remotely)* and the *Staff Manual (clear desk policy information)* which have been provided to the Keeper. Staff are expected to adhere to information security procedures outlined in the *Information and Records Management Handbook* when remote working. All SIC staff are required to undertake mandatory data protection training annually. Paragraph 81 of the *Data Protection Policy and Handbook* lists the initial and refresher training provided to staff. The SIC have separately provided additional, detailed evidence of the annual and refresher training in place. Training on data protection and information security has been included in the induction process for all new members of staff in 2021-22 and 2022-23. All staff are required to undertake mandatory data protection training annually. It has been confirmed this has taken place in 2021-22 and 2022-23. An internal auditor reviewed the effectiveness of the authority's UK GDPR Compliance in 2022 and a summary of the findings in relation to the provision of training has been provided. The Keeper notes that the SIC commit to updating data protection legislation terminology to reflect UK's departure from the EU in policies and procedures at the time of review. In addition, the Keeper welcomes the notification that the SIC will review further potential changes around data protection compliance. The Keeper acknowledges the measures, outlined in the future developments section for this element, which were put in in place during changes to working arrangements as a result of the impact of the Covid-19 pandemic. The Keeper agrees that the Scottish Information Commissioner 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 *RMP* states "The Commissioner's recognises the importance of the recovery of records in the event of an emergency affecting the office premises or systems." This is echoed in *the Information and Records Management Handbook* (paragraphs 47-49), which states the authority's business continuity plan "is designed to protect and provide access to the Commissioner's records in the event of disaster or serious disruption to normal business." The Scottish Information Commissioner has a *Business Continuity Policy* (version 01.05 dated June 2021) and a *Business Continuity Plan* (*BCP*) The Keeper has been provided with a link to the *Policy*, which is published on the authority's website, and an extract of the *BCP*. The Head of Corporate Services (named at element 2) has lead responsibility for BCP implementation. At the time of submission, measures were in place in response to Covid-19 working arrangements and the *Business Continuity Policy* was under review. The Keeper notes these arrangements made provision for records management, including temporary procedures and staff guidance. It has been confirmed separately that the Business Continuity Policy has been kept under review during the course of the COVID-19 pandemic, and that records management arrangements are in place which cover remote working and hybrid working. The *RMP* states that the BCP arrangements cover "•recovery of records made temporarily unavailable due to an unexpected event • accessing records vital to core business activities and include access arrangements for insurance details, business contract information, key contacts, banking arrangements, personnel files, case

			files, etc." The extract of the *BCP* provided shows the contents page, which includes a section on IT recover plan and one on paper records, and the first four pages of the plan. The extract outlines the roles and responsibilities of the Core Recovery Team, which includes the Head of Corporate Services (named at element 2); and phases of recovery, including recovery of IT systems and full access to systems. The *BCP* and *Business Continuity Policy* are designated as key documents and as such undergo regular review (*RMP* page 19). The SIC maintain a register of Key Documents and have a *Key Documents Handbook* which supports the management of this. The *Key Documents Handbook* is published on the authority's website. Internal audit is utilised to carry out periodic audits of business continuity arrangements and testing of elements of the BCP are also periodically tested through BCP exercises (*Business Continuity Policy* paragraphs 14-15). The information security policy statement notes, "Information is a valuable asset and business continuity is dependent on its integrity and continued availability and the Commissioner is committed to the secure use of information and information technology systems in order to protect the availability, integrity and confidentiality of the information under our control." (*Information and Records Management Handbook* section 6) The Keeper agrees that the Scottish Information Commissioner 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 processes in place to track public records in such a way that their location is known and changes recorded.

			The *Records Management Policy* includes among its objectives, "Security: that records are secure from unauthorised or inadvertent alteration, destruction or deletion, that access and disclosure will be properly controlled and audit trails will track all use and changes. Records and the systems in which they are held will be held in a robust format ensuring records remain retrievable and readable for as long as the records are required." In addition, section 4 of the *Policy* states, "The electronic document and records management systems used by the Commissioner log all records activity. This provides an audit trail which can be used as evidential support for system monitoring and compliance auditing." The *RMP* states "The Scottish Information Commissioner has systems and procedures in place to ensure an audit trail exists for the editing, movement and destruction of our records." The *Information and Records Management Handbook* states, "The efficient location and retrieval of information is vital to support the effective running of the organisation and to comply with the requirements of the DPA, UK GDPR, FOISA and the EIRs." (paragraph 139) And "This is achieved through the consistent and rigorous application of naming conventions, the application of version control guidance and by following indexing and storage guidance." (paragraph 140) The *RMP* and *Information and Records Management Handbook* explain the procedures in place for both digital and hardcopy (paper) records. Digital: Virtual Cabinet, VC (corporate records) - This system has a built-in audit log and version control functionality; and view, edit and delete functions are set to reflect the SIC policies and procedures. Indexing is also a mandatory function in VC when creating or moving an existing record. An extract of the Virtual Cabinet destruction

			log sample has been provided to evidence this. Workpro (casework records) - Workpro uses Web Day. The *RMP* states this system incorporates full audit trail; and view, edit and delete functions are set to reflect SIC policies and procedures. Automated version control capability is expected to be included in the next upgrade of the system. It has been confirmed separately that an update was rolled out in August 2022, with regular smaller updates. Network drives – The SIC acknowledge the limitations of using network drives to store records as no automatic version control is available. Certain metadata is available ‘‘which provides an audit trail of creation and the last review of the record.’’ (*IRM Handbook* paragraph 153). Network drives are only used in specific circumstances to store records. Hardcopy: Paper records – A register is used to manage ‘non-investigation’ paper records in VC. Where there is a need for casework hardcopy records, these are managed through the Workpro system, which can record location and the responsible staff member. The records themselves are stored in folders marked with the corresponding information from Workpro. Only in exceptional circumstances would a paper casework record leave the SIC premises. A sample extract paper destruction log has been supplied. It has been confirmed separately that ‘‘The management of paper records has been updated following the move to remote working and hybrid working. As far as possible, paper records are not created or held and all new records should be held electronically and managed via our records management systems using VC and WorkPro. Due to the revised procedures that we now have, there is no paper record register in place for 2023-24.’’ Section 6 of the *Information and Records Management Handbook* addresses version control, naming conventions and indexing. It outlines procedures in place

			and provides staff guidance, specifically for VC and Workpro. The *Investigations Handbook* contains records management guidance on naming documents in Workpro (paragraphs 166-167 and appendix 7). This document is published on the on the authority's website. It also outlines procedures for tracking the location of hardcopy casefiles/information if removed from office premises. Document controls sheets are also in use for all 'key documents'. A sample template has been provided and their use is demonstrated in supporting documents supplied as evidence. The SIC maintain a register of Key Documents and have a *Key Documents Handbook* which supports the management of this. The *Key Documents Handbook* is published on the authority's website The future developments section of this element notes upgrades to several systems were planned for 2021-22. Information about updates to systems since submission has been provided separately. The Keeper agrees the Scottish Information Commissioner 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. In the Commissioner's signed *Covering Statement* he commits to ensuring "• all staff maintain, and develop as necessary, their competence in information and records management" And "• all employees, contractors, agents, consultants and other third parties who have access to any information held within the Commissioner's office, are fully aware of and abide by their information and records management duties under the PRSA."

			The SIC highlight they are a small authority of 25 staff and as such do not have a dedicated records management post. The Keeper fully acknowledges and accepts this is the case for many public authorities. The *Information and Records Management Policy* (section 3) outlines staff records management responsibilities and training. The *Policy* states ‘‘Staff training and support is recognised by the Commissioner as necessary for the successful implementation of this policy.’’ The Keeper welcomes this recognition. The Head of Corporate Services is identified as the individual with operational day-to-day responsibility for records management and implementation of the *RMP*. Records management forms part of the responsibilities of the post-holder. The Head of Corporate Services is supported by staff who also have specific records management responsibilities and duties, the Finance and Administration Manager and Administrator. The *Information and Records Management Handbook* (section 9) contains competencies frameworks for the Head of Corporate Services, Finance and Administration Manager and Senior Management Team, showing records management responsibilities. The *RMP* explains that the Finance and Administration Manager is supported in attending records management training, including PRSA surgeries. The future developments section notes a commitment to considering external records management training for staff with specific records management responsibilities and duties. The *RMP* explains that new staff undertake records management induction training and receive refresher training, for example when systems are updated. Data

			protection training is mandatory for all staff and must be completed annually (see element 9). In addition, staff who deal with personal data receive further training on data protection legislation. The Keeper has been provided, separately, with an extract from the *Model Induction Plan*. The extract outlines the induction training in place and who will carry out the training. This document is also published on the authority's website. It has been confirmed separately that this training is conducted either in-person or using MS Teams. Staff are also required to confirm they have read policies and procedures as part of their induction. The *Information and Records Management Handbook* (section 9) contains a competency framework for all staff which outlines the training they will receive. This comprises induction and in-house training; review of current practice and past experience and performance; on job training; and use of support manuals. All staff are provided with *Information and Records Management Handbook* and required to confirm they have read and understood the *Information and Records Management Policy* and *Handbook* annually. The key responsibilities of the Head of Corporate Services (as outlined in the *Information and Records Management Policy*) include ''provide appropriate training, guidance and feedback mechanisms to support staff in carrying out their records management responsibilities''. The Head of Corporate Services is also responsible for alerting staff to updates of systems. The *RMP* notes that a register of staff records management training is maintained. The Keeper has been provided, separately, with details of the use of personal development plans and provided with a copy of the template used to determine a member of staff's learning and development needs as part of the annual Performance and Development process that is in place. Details of the Learning and Development Plan have also been

			provided. The Learning and Development Plan is approved by the Commissioner and the SMT each financial year and identifies where training is to be provided to a particular member of staff as well as when training is to be provided to all members of staff. As policy, procedure and guidance documents are published online the Keeper can agree staff have access to these. The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, the Keeper agrees that the Scottish Information Commissioner 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. The *Commissioner's Covering Statement* notes, "Information and records management underpins all that the Commissioner's office does and is part of our annual operational planning. An annual assurance report on records management is a mandatory reporting requirement under our Governance Arrangements and is provided by the Head of Corporate Services who has operational responsibility for records management." The *Commissioner's Covering Statement* provides further assurance to the Keeper of the commitment to ongoing assessment and review of the authority's records management provision, "I also recognise that there is always scope to improve and develop what we do and how we do it. I am committed to continuous improvement and to ensuring that our key documents are actively reviewed, including those relating to information and records management and our processes and procedures." The Keeper welcomes and commends these statements in support of this element.

			The *Information and Records Management Policy* lists performance measurement as one its objectives and states "the application of records management procedures are regularly monitored and reviewed, and action taken to improve standards as necessary." Section 4 of the *Policy* relates to performance review and compliance monitoring. The *RMP* is identified as a key document and as such is subject to a formal review by the SMT under a programme of planned reviews. The schedule for planned reviews is considered by the SMT every two months. Any changes to the *RMP* require SMT approval. A link to the published *Key Documents Handbook* has been provided. This document outlines the process for updating key documents and includes records management policies, procedures and guidance. Each key document has a responsible manager. The *Key Documents Handbook* states "A key component of our records management arrangements is our approach to the management of 'Key Documents'."(paragraph 4) The Head of Corporate Services (named at element 2) is responsible for this review. The *Information and Records Management Policy* (section 3) confirms the responsibilities of the post-holder for reviewing and updating the policy and supporting guidance, arranging an annual review and disposal of files, managing the audit programme and ensuing any remedial actions are carried out. The *Information and Records Management Handbook* (section 10) contains an outline of the compliance monitoring arrangements carried out by the Head of Corporate Services. Section 7 of the *Handbook* details the records review procedure under the file plan and retention schedule. This is carried out by Heads of Departments, following the *Records Review Procedure* (see element 6). The Head of Corporate Services is required to provide an annual report to the SMT on records and information management. A link to the published *Governance*

			Reporting Arrangements confirming this has been provided. A link to the published *Information and Records Management Committee Report 2020-21*, submitted by the Head of Corporate Services to the SMT on 12 May 2021 has been provided. This report provides information on the following areas of records management provision and implementation in the authority: • retention and destruction • information security • data protection • appropriate back-up arrangements • management of key documents in line with the Key Documents Handbook It also includes an assessment of the level of compliance with the *Information and Records Management Policy* and the procedures set out in the *Information and Records Management Handbook*. In addition to the above reviews in place, the SIC will undertake periodic information and records management system audits, such as Archives and Records Management Services (ARMS) Quality Improvement Framework online toolkit (*Information and Records Management Policy*, paragraph 31). Document control sheets are used by the authority to show approval information, record changes and planned review dates. As noted above the SIC have arrangements in place for the regular review of key documents, which includes supporting records and information policies and procedures. For example: • *Information and Records Management Policy* (approved 30 June 2021, updated December 2022) planned review July 2023 • *Information and Records Management Handbook* (dated 30 June 2021) planned review July 2024

			• *File Plan and Retention Schedule* (version 02.13 dated March 2019). • *Records Review Procedures* updated December 2022, planned review date July 2023. Internal audit is utilised to carry out periodic audit of business continuity planning arrangements. Areas of the *BCP* are also periodically tested through BCP exercises (*BCP* paragraphs 14-15). Records and information management related activities form part of the SIC Operational Plan 2021-22, a link to the published plan has been provided. The current 2022-23 Operational Plan is also published on the authority's website. An annual information and records management assurance report to the SMT and "coordinate on-going Information and Records Management (IRM) controls and procedures and ensure they are applied" are among the activities included in these plans. The future developments section for this element notes a project to consider and recommend a way forward for the management of key documents and reviews was to take place in 2021-22. It has been confirmed separately that this project has been carried forward to 2023-24. The Keeper agrees that the Scottish Information Commissioner 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, the Keeper agrees that supporting policy and guidance documents have appropriate review periods allocated.
14. Shared Information	**N/A**	**N/A**	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 RMP explains that the SIC do not have any data sharing arrangements in place. An assurance is provided that should this situation alter, information sharing would be undertaken in a necessary, lawful, and controlled manner as required by the Act. The *Data Protection Policy* (paragraphs 43 and 54) confirms the SIC do not have any data sharing agreements in place at present, but that if any such agreement is put in place it should comply with 'Data sharing: a code of practice' issued by the Information Commissioners Office (ICO). The Keeper acknowledges the overview provided in the *RMP* of the authority's publication scheme and Guide to Information, and adoption of the Model Publication Scheme in its entirety and supporting evidence. Plans for improving the Scottish Information Commissioner's website accessibility are outlined in the future developments section. It is stated that any changes will consider records management processes. As part of their functions the SIC deal with investigations under the Freedom of Information (Scotland) Act 2002 (FOISA), Environmental Information (Scotland) Regulations 2004 (the EIRs) and INSPIRE (Scotland) Regulations 2009. This involves the processing of information supplied by third parties on a case-by-case basis rather than scheduled information sharing. As noted above, the Workpro system is used for case management and the process for conducting investigations is detailed in the *Investigations Handbook*. At the time of the Keeper last agreement this element was awarded a green RAG status. Given the information provided, stating that the SIC do not have any data sharing arrangements in place, the Keeper accepts this element is not applicable

			and expects to be informed if this situation should change. The Keeper welcomes the assurance that if this situation should change in the future, measures will be put in place to appropriately manage information sharing.
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). The Scottish Information Commissioner is clear this element of the Keeper's Model Plan is not applicable, "the Commissioner does not delegate any functions to be carried out by third parties." (*RMP* page 32) The Keeper accepts this statement and expects to be informed if this situation should change in the future.

The Scottish Information Commissioner

General notes on submission:

Version: This assessment is on the Scottish Information Commissioner's Records Management Plan (the RMP) submitted to the Keeper for agreement on 30th June 2021. The RMP is version 02.03 dated 30th June 2021, and was approved the Senior Management Team and Commissioner. The RMP contains links to the Scottish Information Commissioner website to access supporting evidence documents. As there has been a delay between the submission date and the assessment, the assessment has been based on the versions of supporting documents accessed through the website in 2023.

The RMP includes a covering statement from the Scottish Information Commissioner, Darren Fitzhenry (named at element 1): "I recognise the value of our records as a corporate asset and records management as a key corporate function. Our records are our corporate memory providing evidence of actions and decisions and supporting our daily functions and operations."

"Information and records management underpins all that the Commissioner's office does and is part of our annual operational planning. An annual assurance report on records management is a mandatory reporting requirement under our Governance Arrangements and is provided by the Head of Corporate Services who has operational responsibility for records management."

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 Keeper previously agreed the RMP of the Scottish Information Commissioner in 2014, Microsoft Word - PRSAassessmentReportScottishInformationCommissioner.rtf (nrscotland.gov.uk)

6. Keeper's Summary

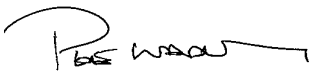
Elements ***1-15*** that the Keeper considers should be in a public authority records management plan have been properly considered by the ***Scottish Information Commissioner***. Policies and governance structures are in place to implement the actions required by the plan.

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper agrees the RMP of **Scottish Information Commissioner.**

- The Keeper recommends that Scottish Information Commissioner should publish its agreed RMP as an example of good practice within the authority and the sector.

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



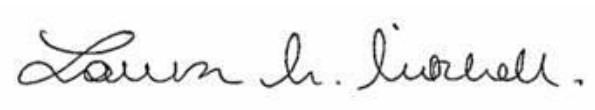
…… ……

Pete Wadley
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 **Scottish Information Commissioner** In agreeing this RMP, the Keeper expects Scottish Information Commissioner to fully implement the agreed RMP and meet its obligations under the Act.



Laura Mitchell
Deputy Keeper of the Records of Scotland