

Public Records (Scotland) Act 2011

Scottish Biometrics Commissioner

The Keeper of the Records of Scotland

13 October 2023

Contents

1. Public Records (Scotland) Act 2011	3
2. Executive Summary	4
3. Authority Background	5
4. Assessment Process	6
5. Model Plan Elements: Checklist	7-36
6. Keeper's Summary	37
7. Keeper's Determination	38
8. Keeper's Endorsement	39

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 Biometrics Commissioner by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 28 February 2023.

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

3. Authority Background

The Scottish Biometrics Commissioner Act 2020 established the office of Scottish Biometrics Commissioner and provides for its functions. The Commissioner is independent of Scottish Government and is appointed by Her Majesty the Queen on the nomination of the Scottish Parliament.

The Commissioner's general function is to support and promote the adoption of lawful, effective, and ethical practices in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes by Police Scotland, the Scottish Police Authority (SPA), and the Police Investigations and Review Commissioner (PIRC).

The Commissioner must lay an annual report on activities each year before the Scottish Parliament and may publish other reports and research, as necessary.

[Scottish Biometrics Commissioner | Responsibility for Biometric Data in the Criminal Justice and Policing Sector | Scottish Biometrics Commissioner](#)

The current Strategic Plan is published on the authority's website [Scottish Biometrics Commissioner 4-Year Strategic Plan 2021-2025 \(For period 01/12/2021-2025\)](#)

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 Biometrics 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	<p>The Public Records (Scotland) Act 2011 (the Act) requires that an individual senior staff member is identified as holding corporate responsibility for records management in a public authority.</p> <p>The Scottish Biometrics Commissioner (SBC) have identified Dr Brian Plastow as holding corporate responsibility for records management in the authority. Dr Plastow holds the position of Scottish Biometrics Commissioner. The Records Management Plan (<i>RMP</i>) states “The Commissioner has overall strategic accountability for records management and accepts overall responsibility for the Records Management Plan that has been submitted.”</p> <p><i>A Statement from the Commissioner</i> (dated 3 February 2023) has been provided to the Keeper of the Records of Scotland (the Keeper) in support of the <i>RMP</i> and specifically confirming arrangements around elements 2 and 15.</p> <p>This identification is further supported in the <i>Records Management Policy within SBC Information Governance Handbook</i> (version 2.0 dated July 2023), a link to which has been provided. Roles and responsibilities are outlined on pages 6-7. A copy of the <i>Commissioner’s job description</i> has also been provided.</p> <p>The Commissioner reviewed the <i>RMP</i>, and the following documents submitted as evidence to support it, <i>SBC Information Governance Handbook</i> and <i>Records Management Self-Assessment Checklist</i> (version 1.0 dated February 2023).</p>

			<p>The Keeper agrees that the Scottish Biometrics Commissioner have identified an appropriate individual to this role as required by the Act.</p>
<p>2. Records Manager</p>	<p>G</p>	<p>G</p>	<p>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.</p> <p>The Scottish Biometrics Commissioner have identified Cheryl Glen, Corporate Services Manager, as the individual holding operational responsibility for records management in the authority. The <i>RMP</i> states “The Corporate Services Manager is responsible for day-to-day records management; for the implementation of the SBC’s Records Management Plan and the activities described in the elements. The Corporate Services Manager is the Keeper’s initial point of contact for records.” The Corporate Services Manager is also identified under elements 1 to 14 of the <i>RMP</i> as either the sole responsible officer or one of the named responsible officers.</p> <p><i>A Statement from the Commissioner</i> supports this identification. It also makes a commitment to providing ongoing support for all staff in accessing training and development around records management. The Keeper commends this commitment to records management training.</p> <p>A copy of the <i>Corporate Services Manager job description</i> has been provided. This confirms the postholder’s records management responsibilities and that the post reports directly to the Commissioner (named at element 1). It also notes the postholder manages the Business Support Officer, who also has records management responsibilities.</p> <p>The Corporate Services Manager is supported by the Business Support Officer, whose job description has been provided and which includes specific records</p>

			<p>management competency requirements and responsibilities.</p> <p>This identification is further supported in the <i>Records Management Policy within SBC Information Governance Handbook</i>, a copy of which has been provided. Roles and responsibilities are outlined on pages 6-7.</p> <p>The Corporate Services Manager prepared the <i>RMP, SBC Information Governance Handbook</i> and <i>Records Management Self-Assessment Checklist</i>; and is the author of the <i>File Plan</i> (version 2.0 dated January 2023) and <i>File Type Guidance</i> (version 2.0 dated January 2023).</p> <p>A commitment is made in the <i>RMP</i>, under the assessment and review section, to monitor and review annually the training and development needs of staff with records management responsibilities. The <i>RMP</i> (page 19) notes the intention to use annual performance and development appraisals to assess training needs. The Keeper commends this commitment to ensuring staff have access to appropriate training and skills development. See element 12 for comments on staff training.</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner have identified an appropriate individual to this role as required by the Act.</p>
3. Policy	G	G	<p>The Act requires an authority to have an appropriate policy statement on records management.</p> <p>The <i>Records Management Policy</i> is located in the <i>Information Governance Handbook</i>. It includes the following statement, “Records are a vital information asset and a valuable resource for the organisation's decision-making processes, policy creation and operations and must be managed effectively from the point of their creation until their ultimate disposal.” (page 4)</p>

			<p>The <i>Records Management Policy</i> is applicable to all SBC staff and covers all records created or managed by the authority. It outlines the authority’s objectives and commitments, staff roles and responsibilities and mentions the requirements of the Public Records (Scotland) Act 2011 (the Act) (pages 4-5). In addition, records management training is specifically addressed (page 6).</p> <p>The <i>RMP</i> states “SBC recognises that the effective management of our records is essential in order to support our functions, to comply with legal, statutory and regulatory obligations and to demonstrate transparency and accountability to all of our stakeholders.” It also notes that the SBC complies with Section 61 Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002.</p> <p>The <i>Policy</i> is subject to ongoing review and will be reviewed in line with the <i>RMP</i>. It is the responsibility of the Corporate Service Manager (named at element 2) to monitor compliance with the <i>Policy</i> (<i>Information Governance Handbook</i> page 7).</p> <p>Since submission the <i>Information Governance Handbook</i> (version 2.0 dated July 2023) has been published on the SBC website, Information Scottish Biometrics Commissioner. The Keeper can agree that the <i>Records Management Policy within SBC Information Governance Handbook</i> is accessible to staff and the Commissioner.</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner has a formal records management policy statement as required by the Act.</p>
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.

			<p>The <i>Records Management Policy</i> notes “Through the effective management of the organisation’s records, the SBC can provide a comprehensive and accurate account of its activities and transactions.” And commits to “The maintenance of a Business Classification Scheme (BCS) to reflect the functions, activities and transactions of the SBC.”(<i>Information Governance Handbook</i> pages 4- 6)</p> <p>The SBC create and manage their public records digitally using the Scottish Government (SG) electronic records and document management system (eRDMS), Objective, through the SCOTS network. The eRDMS is configured to the SG BCS and the SBC have a separate file plan within the system in which the authority’s <i>File Plan</i> and BCS is implemented. The Keeper is familiar with the Objective system and its records management functionality. A <i>Screenshot of eRDM Folder and File Structure - January 2023</i> has been provided separately.</p> <p>The SBC have a functional <i>File Plan</i> and BCS in place to manage their public records. It is noted that the <i>File Plan</i> has an excluded data section which states, “The Scottish Biometrics Commissioner when conducting audits, inspections, or reviews of biometric data records held by one of the bodies to whom the Commissioner’s jurisdiction extends will not under any circumstances replicate any personal biometric data onto eRDM. Where review notes are taken as part of an audit, review, or inspection of such bodies, or as part of the investigation of a complaint relating to the Code of Practice, those notes will be destroyed immediately once the factual accuracy of the content of any report has been agreed with relevant stakeholders and our findings report published.” The <i>RMP</i> states the BCS “is modelled on the functions of the organisation and directly reflects the hierarchical relationship of functions, activities, transactions and records.” The Keeper commends the use of a functional system which is considered best practice.</p> <p>Copies of the <i>File Plan</i> and <i>Business Classification Scheme (BCS) within SBC Information Governance Handbook</i> have been supplied as evidence. The <i>File Plan</i></p>
--	--	--	--

			<p>is also published on the SBC website, Information Scottish Biometrics Commissioner.</p> <p>The <i>Business Classification Scheme (BCS)</i> section of the <i>Information Governance Handbook</i> explains the structure of the file plan and BCS and notes the SBC recognise “Electronic record and document management needs to be very carefully considered and structured to ensure the integrity of the documents is not compromised upon capture and they remain retrievable for as long as they are required.”</p> <p>The <i>Information Governance Handbook</i> includes procedures and staff guidance on the administration of the eRDMs and file management guidance. This provides instruction on where to create and store records, for example “▪ all documents will be filed electronically within eRDM ▪ documents must not be stored anywhere other than eRDM”.</p> <p>The <i>File Plan</i> (page 5) directs staff to SG guidance on use of the eRDMs through the SG intranet site.</p> <p>The <i>RMP</i> explains the SBC operate a paperless office and do not create hardcopy records (pages 8,10 and 18). It notes there is a <i>Shared Services Agreement</i> in place with support services for financial processing and human resources management provided by the Scottish Public Services Ombudsman (SPSO). This agreement is approved by the Parliament Corporation and a copy has been supplied to the Keeper. The SBC staff do not have access to any paper records created by the SPSO. The Keeper has previously agreed the records management arrangements of the SPSO.</p> <p>There is however reference to hardcopy records when dealing with the complaints process in the <i>Information Governance Handbook</i> (File Management Guidance,</p>
--	--	--	--

			<p>page 12), “when complaints are closed, no further hardcopy documents should be stored, all new documents should be stored on the electronic file only, through scanning if necessary.” Annex 2 of the <i>Data Protection Policy and Procedures</i> sets out staff guidance on confidentiality, security, data recording and storage and notes “Physical files are securely locked away within the office until destroyed. All work is stored on eRDM.” (<i>Information Governance Handbook</i> page 60).</p> <p>The Keeper acknowledges that the SBC receive hardcopy records during the complaints and review process. The Keeper acknowledges that the secure storage and destruction of such records is explained.</p> <p>An Information Management Support Officer (IMSO) is in place to assist with the management of records in the eRDMs and receives additional training. The Business Support Officer (see element 2) is the IMSO (<i>Governance and Risk Management Handbook</i>). The responsibilities of the IMSO are outlined in the <i>Information Governance Handbook</i> (pages 10-11).</p> <p>The SBC use the SG email system which automatically manages email retention and disposal through the Enterprise Vault system (<i>RMP</i> pages 9-10). The Keeper is aware that Enterprise Vault is being replaced in the Summer of 2023. SG guidance and training on information management includes the use of eRDMs and how to save emails which are to be retained.</p> <p>The <i>File Plan</i> is reviewed and updated to meet the business needs of the authority, “The management of SBC records and the BCS are subject to ongoing monitoring and annual reviews to ensure that all of the functions, activities and transactions carried out by the SBC continue to be accurately represented within it.” (<i>RMP</i> page 8)</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner retains all its public</p>
--	--	--	---

			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	<p>The Keeper expects an authority to have allocated retention periods to its public records and for those records to be retained and disposed of in accordance with a Retention Schedule.</p> <p>The <i>Records Management Policy</i> commits to "The review of the retention and disposal policy to provide clear guidance regarding the management of SBC records and the correct procedures to follow when disposing of business information" (<i>Information Governance Handbook</i> page 6).</p> <p>The SBC have a retention and disposal schedule in place, <i>File Type Guidance – Retention and Disposal</i>. A link to which has been provided. This document is published on the SBC website, Information Scottish Biometrics Commissioner. It identifies file types for the authority’s public records and outlines the retention and disposal actions for each.</p> <p>The <i>File Type Guidance – Retention and Disposal</i> is based on SG guidance as the SBC use the SG eRDMs. The retention and disposal schedule is in line with the SG BCS which has standard file types in place.</p> <p>Automatic retention and disposal actions are allocated to each file type in the eRDMs. The Keeper agrees that the SG eRDMs appropriately imposes retention periods and agreed in 2022 that this system is suitable for the management of public records.</p> <p>A <i>Retention and Disposal Policy</i> is contained within the <i>Information Governance Handbook</i>. It states its aim is “to identify documents which should be retained because of their legal, statutory and regulatory obligations, or long-term</p>

			<p>historical/research value and enable the SBC to dispose of documents promptly when they cease to be of any continuing administrative/legal value.”</p> <p>The <i>Retention and Disposal Policy</i> explains how retention decisions have been developed in line with legislation, best practice, and business needs. Section 8 of the <i>Publication Scheme</i> states, “Our ICT Platform is supplied under contract to Scottish Government, although we have developed our own Records Management And Retention and Disposal Policies”. This indicates the authority has been involved in the allocation of retention decisions.</p> <p>The IMSO (see element 4) is responsible for “reviewing Scottish Government reports for retention and disposal of documents and providing advice on information management to colleagues.” (<i>Information Governance Handbook</i> page 11)</p> <p>The SBC use the SG email system which automatically manages email retention and disposal through the Enterprise Vault system (<i>RMP</i> pages 9-10).</p> <p>The Keeper can agree staff can access the <i>File Type Guidance - Retention and Disposal</i> and <i>Information Governance Handbook</i> as they are published on the authority’s website.</p> <p>The further developments section in the <i>RMP</i> notes the SBC are developing a separate disposal policy for the manual deletion of records relating to specific complaints to ensure personal data is deleted within a set time frame. The Keeper commends this development and would like to be provided with sight of the policy, or evidence of its development and commitment to implementation. See element 6 for further comment.</p> <p>The retention schedule will be kept under review and SBC recognise this is necessary to ensure it continues to meet business needs (<i>RMP</i> page 9).</p>
--	--	--	---

			<p>The Keeper agrees that the Scottish Biometrics Commissioner has a schedule providing retention decisions for the record types created while pursuing its functions.</p>
<p>6. Destruction Arrangements</p>	<p>A</p>	<p>G</p>	<p>The Act requires that public records are destroyed in a timely, controlled and secure manner.</p> <p>The SBC have a retention and disposal schedule in place. A link to <i>File Type Guidance – Retention and Disposal</i> has been provided. This document is published on the SBC website, Information Scottish Biometrics Commissioner. It identifies file types for the authority’s public records and outlines the retention and disposal actions for each.</p> <p>As the SBC use the SG eRDMs, the destruction of digital records from the system is an automated process managed by SG policies. The file types assigned to the SBC public records in the eRDMs have set retention and disposal periods. As the SBC are a new authority it is unlikely any records will have reached their retention period yet. The Keeper is familiar with the eRDMs and understands that when records are destroyed a record of destruction is created and retained permanently.</p> <p>The <i>RMP</i> explains that manual deletion may also be conducted in line with the retention and disposal policy and that this process will be managed by the Corporate Services Manager (named at element 2) with the assistance of the Business Support Officer. As noted above, the Business Support Officer is the authority’s IMSO and will review SG reports on retention and disposal. A copy of the Business Support Officer <i>job description</i> has been provided which includes managing information and records among the responsibilities of the role.</p> <p>As noted at element 5, the SBC are developing a separate disposal policy for</p>

			<p>specific complaint records which will be manually deleted. The Keeper wishes to be updated on this work and provided with sight of the policy, or evidence of its development and commitment to implementation. The SBC have confirmed separately that they will update the Keeper on this work. Updates can be provided through the annual Progress Update Review (PUR) process, Progress Update Reviews National Records of Scotland (nrscotland.gov.uk).</p> <p>The SBC use Microsoft Exchange and Enterprise Vault for email management and disposal. Enterprise Vault manages the automatic destruction of email. As noted above, this will be replaced later in 2023. The Keeper is satisfied that the replacement system will provide similar auto-destruction capabilities albeit with a more generous run-up period.</p> <p>The SBC do not create hardcopy records. They have explained that any paper records received are digitally scanned and then securely destroyed through the paper shredding services in place at the SPSO. Details of procedures for the destruction of paper records at SPSO, supplied by Paper Shredding Services (PSS), have been provided. The Keeper has previously agreed that the SPSO have appropriate processes in place for the destruction of paper records.</p> <p>It has been confirmed separately that prior to the SBC taking on the destruction of hardware themselves, this was offered by SPSO through the Shared Services Agreement, and has been previously utilised. The Keeper has previously agreed that the SPSO have appropriate processes in place for the destruction of hardware. A copy of the <i>SPSO Information Governance Handbook</i>, which includes their RMP and a section on the destruction of hardware, has been provided separately. However, the Keeper understands that SBC have since taken over responsibility for the destruction of hardware from SPSO although it is unlikely that the SBC will have destroyed any hardware since this change. The further developments in the <i>RMP</i> (page 10) explains how this will be conducted when required, including ensuring set</p>
--	--	--	---

			<p>standards are met and a record of destruction is produced. The authority intends to manage this through contractual agreements with suppliers. Since submission, the SBC have noted they will update the Keeper with arrangements for hardware destruction. The Keeper welcomes this commitment and can be updated and provided with evidence to show this is operational through future PUR submissions.</p> <p>As the SBC use the SG SCOTS network, the Keeper can agree appropriate arrangements are in place for the irretrievable destruction of backups after a known period. A copy of the <i>ITECS ICT SCOTS Connect services Terms of Supply</i> (dated September 2022), which outlines back-up procedures, has been provided. The Keeper agreed the SG destruction arrangements in 2022.</p> <p>The Keeper can agree this element on an ‘improvement model’ basis as the Scottish Biometrics Commissioner have identified a gap in provision (updated operational procedures are not yet in place for the secure destruction of hardware) and have provided an outline of how this is to be addressed using contracts with suppliers. In addition, a separate disposal policy for specific records which will involve the manual deletion of records is being developed. The Keeper can be updated on both these areas of work and provided with evidence, for example sample contracts and destruction certificates, through the PUR process.</p>
7. Archiving and Transfer	G	G	<p>The Act requires that all Scottish public authorities identify a suitable repository for the permanent preservation of any records considered suitable for archiving. A formal arrangement for transfer to that repository must be in place.</p> <p>An acknowledgement of the enduring value of the public records of the Scottish Biometrics Commissioner is included in the <i>Retention and Disposal Policy</i></p>

			<p>(<i>Information Governance Handbook</i> page 1), “This retention and disposal policy aims to identify documents which should be retained because of their legal, statutory and regulatory obligations, or long-term historical/research value and enable the SBC to dispose of documents promptly when they cease to be of any continuing administrative/legal value.”</p> <p>The SBC have identified National Records of Scotland (NRS) as the proper repository for the small selection of their public records suitable for permanent preservation.</p> <p>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.</p> <p>The SBC have a formal agreement in place with NRS that governs the transfer of records. A copy of the <i>Agreement for the Transfer of Records</i>, signed in February 2023, has been provided as evidence.</p> <p>Records for transfer to NRS are identified in the <i>File Type Guidance – Retention and Disposal</i>. The <i>RMP</i> (page 12) notes “NRS had an opportunity to contribute to the SBC records retention schedule through the File Plan which identifies the records selected for permanent preservation.”</p> <p>The IMSO (see element 4) is responsible for “reviewing Scottish Government reports for retention and disposal of documents and providing advice on information management to colleagues.” (<i>Information Governance Handbook</i> page 11) The Corporate Services Manager is listed as the responsible officer for element 7 of the <i>RMP</i>.</p> <p>The <i>NRS Agreement for the Transfer of Records</i> also includes the archiving of the</p>
--	--	--	--

			<p>SBC website. The <i>Retention and Disposal Policy</i> makes the statement “Published documents are contained on the SBC website. The SBC website is to be listed with the NRS web archive whose purpose is to give permanent online access to key websites for future generations and this provides for permanent retention of those documents.” (<i>Information Governance Handbook</i> page 14)</p> <p>The Keeper can agree that the Scottish Biometrics Commissioner have identified a suitable repository for the permanent preservation of any records considered suitable for archiving, and that a formal arrangement for transfer to that repository is in place.</p>
<p>8. Information Security</p>	<p>G</p>	<p>G</p>	<p>The Act requires that public records are held in accordance with information security compliance requirements.</p> <p>The <i>Records Management Policy</i> statement commits to "The review of information security policies and procedures in order to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction". (<i>Information Governance Handbook</i> page 6)</p> <p>The SBC have measures in place to ensure they “comply with the security and access requirements of the Section 61 Code of Practice: Records Management.” (<i>RMP</i> page 13).</p> <p>Information risk is captured and managed through a Strategic Risk Register (<i>RMP</i> page 13). This document is published on the SBC website, Information Scottish Biometrics Commissioner.</p> <p>Information security procedures and guidance are outlined within the <i>Information Governance Handbook</i>. These include a <i>Clear Desk and Screen Policy</i>, <i>Complying with Information Legislation</i>, <i>Protective Marking System</i>, <i>Records Management</i> and</p>

			<p><i>Security Guidance: sharing information off-network and out-of-office, and Protocol for data security incidents.</i></p> <p>The SCB uses the SG SCOTS Connect services to host network services. The public records of the SBC are managed digitally on the SG eRDMS. These systems and access to them are subject to the information security measures of the SG. A copy of the <i>ITECS ICT SCOTS Connect services Terms of Supply</i> has been provided. The Keeper agreed in 2022 that the SG have appropriate information security measures in place. In addition, where necessary the SBC will restrict access to files in the eRDMS to certain staff members (<i>Information Governance Handbook</i> page 9).</p> <p>The Keeper has been separately provided with a copy of the <i>ICT Shared Services Handbook</i> which contains a shared ICT Strategy and IT Security Policy with the SPSO. The Keeper has previously agreed that SPSO have appropriate information security measures in place.</p> <p>Staff guidance is available for situations when working outwith the “SBC secure workspaces”, namely outwith the SG SCOTS network (<i>Records Management and Security Guidance: sharing information off-network and out-of-office</i>). The guidance covers both digital and hardcopy records. While the SBC operate a paperless office, this guidance covers the security of hardcopy records in instances these have been printed off. In such cases a record of movement is maintained by the Business Support Officer.</p> <p>Staff are subject to pre-employment checks, including Disclosure Scotland and must complete eRDMS training before being given access. The <i>RMP</i> explains staff must carry out training in data protection and security awareness training.</p> <p>Physical information security arrangements in place including building security</p>
--	--	--	---

			<p>arrangements and a <i>Clear Desk and Screen Policy</i>. The <i>RMP</i> (page 13) explains the office building used by the SBC meets the SG requirements for the SCOTS network. The <i>Clear Desk and Screen Policy</i> commits to staff information security training and making this part of staff induction training (<i>Information Governance Handbook</i> page 28).</p> <p>Information security and personal data breach reporting procedures are in place and guidance relating to this is included in the <i>Records Management and Security Guidance: Information sharing off-network or when out of office, Protective Marking System, Data Protection Policy and Procedure, and Protocol for Data Security Incidents</i> (<i>Information Governance Handbook</i> pages 27, 32, 59-60 and 71-72).</p> <p>The SBC use a protective marking system for documents and staff guidance on this is contained in the <i>Protective Marking System</i> section of the <i>Information Governance Handbook</i>.</p> <p>The <i>Information Sharing Policy</i> within the <i>Information Governance Handbook</i> provides guidance for securely sharing information (pages 16-21).</p> <p>Annex 2 of the <i>Data Protection Policy and Procedures</i> sets out staff guidance on confidentiality, security, data recording and storage.</p> <p>The <i>SBC Hybrid Working Policy</i> within <i>Working for SBC Handbook</i> addresses information security and confidentiality and directs staff to the <i>Information Governance Handbook</i>.</p> <p>While SG networks, on which the SBC public records are managed, are accredited to the National Cyber Security Centre's Cyber Essentials Plus level, the Keeper welcomes the planned action that the SBC will work towards achieving Cyber Essentials certification. It is noted that since submission this has now been achieved</p>
--	--	--	--

			<p>(certificate dated 4 April 2023).</p> <p>The policies and procedures which support information security measures are subject to ongoing monitoring and review (<i>RMP</i> page 14). The Keeper is pleased to hear that the SBC intend to include information security provision as part of their internal audit activities. The Keeper would welcome updates on this through the PUR mechanism.</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner have procedures in place to appropriately ensure the security of their records as required by the Act.</p>
9. Data Protection	G	G	<p>The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law.</p> <p>The <i>Records Management Policy</i> statement commits to "The review of data protection policies in order to demonstrate the SBC's commitment to compliance with the data protection legislation and the safeguarding and fair processing of all personal data held". (<i>Information Governance Handbook</i> page 6)</p> <p>The Scottish Biometrics Commissioner is a registered data controller with the Information Commissioner's Office (ICO). Details of their ICO registration have been provided (registration number ZB298978, date registered 9 February 2022). This is confirmed in the <i>Complying with Information Legislation (Information Governance Handbook</i> page 43).</p> <p>The SBC have an assigned Data Protection Officer (DPO). The <i>Information Governance Handbook</i> and ICO data protection register entry confirm the Scottish Parliamentary Corporate Body (SPCB) provides a DPO service to the SBC. This arrangement is managed through a MoU (signed June 2022), a copy of which has been provided. The Keeper has previously agreed that SPCB have arrangements in</p>

			<p>place that allow them to properly comply with data protection legislation. The name of the current SPCB DPO is published online and contact details are available on the SBC website.</p> <p>The SBC have a <i>Data Protection Policy and Procedures</i> within in the <i>Information Governance Handbook</i> (pages 46-68). The <i>Policy</i> states the SBC “recognises the importance of privacy by design and the correct and lawful treatment of personal data” and is “committed to compliance with the requirements of the UK GDPR and the DPA (Data Protection Legislation)”. It also commits to providing staff training and guidance.</p> <p>The <i>Data Protection Policy and Procedure</i> and <i>Complying with Information Legislation (Information Governance Handbook</i> pages 42 and 47) outline the data protection principles.</p> <p>Information about making a Subject Access Request (SAR) is included in the <i>Publication Scheme</i> document (pages 13-14) (version 3.0, dated July 2023) which is published on the SBC website, Information Scottish Biometrics Commissioner.</p> <p>The SBC have a <i>Privacy Notice</i> (updated January 2022, link added to SAR information July 2023) published on the their website, Scottish Biometrics Commissioner Privacy Notice Scottish Biometrics Commissioner. It includes information about how the public can exercise their data protection rights and contact details for the DPO.</p> <p>Staff guidance on dealing with SARs is outlined in Annex 4 of the <i>Data Protection Policy and Procedures</i>.</p> <p>The <i>RMP</i> explains that Data Protection Impact Assessments (DPIAs) are used. Procedures and staff guidance are outlined in the <i>Data Protection Policy and</i></p>
--	--	--	--

			<p><i>Procedures and Data Protection Impact Assessments</i> sections of the <i>Information Governance Handbook</i>.</p> <p>The <i>RMP</i> explains there is a separate policy specifically relating to SBC staff personal data which is included in <i>Managing Personal Data Policy (Working for the SBC Handbook)</i>.</p> <p>Annex 1 of the <i>Data Protection Policy and Procedures</i> sets out staff responsibilities, training, and non-compliance actions. The Corporate Services Manager (named at element 2) is responsible for the policy, guidance and ensuring staff undertake training and monitoring this.</p> <p>Mandatory data protection training must be completed annually by all SBC staff and also forms part of induction training (<i>Information Governance Handbook</i> page 56 and <i>RMP</i> page 13). In addition, the MOU with SPCB/DPO includes a provision for awareness raising and staff training.</p> <p>Annex 2 of the <i>Data Protection Policy and Procedures</i> sets out staff guidance on confidentiality, security, data recording and storage. Annex 3 provides staff guidance on protecting personal data.</p> <p>The <i>Information Sharing Policy</i> within the <i>Information Governance Handbook</i> provides guidance on the sharing of personal data in line with data protection legislation.</p> <p>As noted at elements 5 and 6, the SBC are developing a disposal policy for specific complaint records which will be manually deleted to ensure personal data is destroyed within a specified timeframe.</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner have arrangements</p>
--	--	--	---

			<p>in place that allow them to properly comply with data protection legislation.</p>
<p>10. Business Continuity and Vital Records</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.</p> <p>The <i>Records Management Policy</i> statement commits to "The review of the Business Continuity Plan encompassing strategies to ensure vital records held by the SBC remain accessible over time and there are processes in place to monitor the integrity and usability of records" (<i>Information Governance Handbook</i> page 6).</p> <p>The SBC have a <i>Business Continuity Plan (BCP)</i> (version 1, dated February 2022), a redacted copy of which has been provided.</p> <p>The <i>BCP</i> includes an incident response plan, disruption to work arrangements, and staff roles and responsibilities are outlined. The Commissioner (named at element 1), the Corporate Services Manager (named at element 2) and the Business Support Officer are part of the Incident Response Team.</p> <p>The public records of SBC are held on systems operated by the Scottish Government and therefore the authority rely on the back-up/recovery processes of the SG. The SBC <i>BCP</i> (page 5) refers to the iTECS Business Continuity Plan (BCP). The Keeper has previously agreed that SG has appropriate business continuity arrangements in place for the retrieval of records in an emergency. A copy of <i>iTECS ICT SCOTS Connect services Terms of Supply</i> has been provided which outlines back-up arrangements in place.</p> <p>As the SBC have a shared services agreement in place with the SPSO, which includes ICT support, the SPSO ICT department will provide support, for example in the case of cyber security incidents or concerns (<i>BCP</i> page 14).</p>

			<p>The <i>BCP</i> (page 4) notes that each SBC team member has access to a hardcopy of the BCP and an electronic copy is also accessible to the SPCB.</p> <p>The Keeper welcomes the further developments planned for reinforcing business continuity arrangements, including reviewing the <i>BCP</i> following a Business Impact Assessment (BIA), and undertaking a test exercise of the measures put in place. The <i>RMP</i> also notes the Corporate Services Manager is planning to work towards business continuity accreditation. This is commended by the Keeper and updates on this work can be provided through the PUR process.</p> <p>The SBC business continuity documentation will be reviewed annually, and BIAs undertaken as required for new processes or changes to business operations or functions (<i>RMP</i> page 17). The Keeper is pleased to hear that the SBC intend to include business continuity provision as part of future internal audit activities. The Keeper would welcome updates on this through the PUR mechanism.</p> <p>The Keeper agrees the Scottish Biometrics Commissioner have an approved and operational business continuity process and that information management and records recovery properly feature in the authority’s plans. The Keeper acknowledges that all systems in use by the Scottish Biometrics Commissioner are covered under the business continuity arrangements of the Scottish Government.</p>
11. Audit trail	G	G	<p>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.</p> <p>The <i>Records Management Policy</i> states “Through the effective management of the organisation’s records, the SBC can provide a comprehensive and accurate account of its activities and transactions. This may be achieved through the management of effective metadata as well as the maintenance of comprehensive audit trail data.” (<i>Information Governance Handbook</i> page 5)</p>

			<p>The public records of the Scottish Biometrics Commissioner are all digital and managed on the Scottish Government’s eRDMs (Objective). This system has built in audit trail functionality and an effective search function The Keeper agreed in 2022 that this system is suitable for the management of public records.</p> <p>While there is a powerful search function and version control is automated within the eRDMs, naming conventions are required to ensure records can be located. The SBC have naming convention guidance in place. This guidance is found in the Business Classification section of the <i>Information Governance Handbook</i> (page 10) and in the <i>File Plan</i> (pages 5-6). One of the roles of the IMSO (see element 4) is to check naming convention guidance is being followed by staff in the eRDMs.</p> <p>Version control guidance is included in the <i>Data Protection Impact Assessments</i> section of the <i>Information Governance Handbook</i> (page 70). In addition, document control information tables, which include the version number, are shown at the start of the SBC documents.</p> <p>While the SBC operate a paperless office, guidance is included to cover the movement of hardcopy records in the instances these have been printed off. In such cases a record of movement is maintained by the Business Support Officer (who is also the IMSO) (<i>Information Governance Handbook</i>, pages 25-26).</p> <p>The Keeper can agree that the Scottish Biometrics Commissioner has procedures in place that will allow them to locate their records and assure themselves that the located record is the correct version.</p>
12. Competency Framework	G	G	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.

<p>for records management staff</p>			<p>The Scottish Biometrics Commissioner is a small authority, currently comprising the Commissioner and three staff members. The <i>Statement from Commissioner</i>, provided as evidence, makes the following commitment “As Commissioner, I confirm my commitment to providing and supporting access to training and development around records management to all staff, and on an ongoing basis.” The Keeper welcomes and commends this statement.</p> <p>This commitment is echoed in the <i>Records Management Policy</i> statement which commits to “The identification of records management as a distinct stream within the organisation’s training portfolio, with dedicated training provided to all staff.” (<i>Information Governance Handbook</i> page 6). It is further noted in the Learning and Development section of the <i>Working for SBC Handbook</i>, which explains that a yearly report on training and development activities will be produced which will inform future training planning.</p> <p>As the SBC manage their records using the SG eRDMS through SCOTS network, mandatory training is required for all staff before they are permitted access to these systems. This includes eRDMS training and e-learning data protection training. The SBC staff can access this training and guidance on the use of eRDMS and through the SG intranet. One of the responsibilities of the IMSO (see element 4) is to support new staff in completing eRDM - introduction e-learning for new staff (<i>Information Governance Handbook</i> page 11).</p> <p>The <i>Records Management Policy</i> notes “A comprehensive training programme is provided to all staff in order to highlight and increase awareness of their responsibilities in line with data protection, freedom of information and records management.” (<i>Information Governance Handbook</i> page 7).</p> <p>The appointed IMSO (the SBC Business Support Officer) has access to additional training and guidance to enable them to fulfil this role. Again, this is accessed</p>
-------------------------------------	--	--	---

			<p>through the SG intranet.</p> <p>As noted at element 2, job descriptions for the Corporate Services Manager (named at element 2) and the Business Support Officer have been provided.</p> <p>The Assessment Team can confirm the SBC staff attendance at PRSA surgeries and can accept the Corporate Services Manager attendance at SG-led eRDM webinars. The Keeper commends attendance at PRSA events and SG training.</p> <p>It is the Corporate Service Manager’s responsibility to provide staff with records management guidance (<i>Information Governance Handbook</i> page 14) and to monitor the completion of training (<i>RMP</i> pages 6 and 19).</p> <p>The <i>RMP</i> (page 6) notes “Training and development needs are monitored and reviewed annually to ensure post-holders with records management responsibilities have the necessary skills and experiences to carry out their tasks.” The further developments section of the <i>RMP</i> (page 19) notes the intention to use annual performance development reviews to monitor training needs. The development of appraisal procedures is also noted in the Learning and Development section of the <i>Working for SBC Handbook</i>. The Keeper welcomes this planned development and can be updated through the annual PUR mechanism.</p> <p>Training on certain policies, such as the <i>Clear Desk and Screen Policy</i>, and data protection policies and procedures, is noted as being included as part of staff induction training in the <i>Information Governance Handbook</i> page 28, 46, 51 and 54).</p> <p>As noted at element 3, the Keeper can agree that the <i>Information Governance Handbook</i>, which is published on the authority’s website, is accessible to staff and the Commissioner.</p>
--	--	--	---

			<p>The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, the Keeper agrees that the Scottish Biometrics Commissioner consider information governance training for staff as required.</p>
<p>13. Assessment and Review</p>	<p>G</p>	<p>G</p>	<p>Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.</p> <p>The Scottish Biometrics Commissioner will "... review the Records Management Plan and all its elements, at least annually but also when any new operational developments occur to ensure that it remains fit for purpose as part of the internal records management processes..." (<i>RMP</i> page 20)</p> <p>The <i>Records Management Policy</i> statement commits to "The completion of a self-assessment review, following the implementation of the records management plan in order to ensure that the records management practices remain fit for purpose and continue to act as exemplars within the profession in Scotland." (<i>Information Governance Handbook</i> page 6)</p> <p>Reviews will be carried out through the use of a <i>Self-assessment checklist</i>. A copy of the checklist has been provided (version 1, dated February 2023).</p> <p>The <i>Self-assessment checklist</i> comprises 37 questions which address areas of the <i>RMP</i> and states, "This checklist relates to all staff of the SBC and all records created or acquired in the course of its business. It relates to the management of records as an internal facilitative function of the organisation. This checklist is designed to assess the Records Management Plan for the SBC, which details the current record-keeping practices in place within the organisation. The purpose of this checklist is to enable SBC staff to assess the adequacy of the organisation's records management systems and procedures and provides recommendations for action to address any gaps".</p>

			<p>The Corporate Services Manager (named at element 2) will be responsible for overseeing the review process. The <i>RMP</i> explains that staff with relevant responsibilities will be required to complete the checklist. The results and recommendations will be "... shared, actioned and monitored through monthly management team meetings. The monthly and quarterly strategic management meetings include a Governance standing agenda item which includes updates and reviews re policies to be discussed, with any actions being recorded in an action log then discussed/updated at the next meeting." (<i>RMP</i> page 20)</p> <p>The reporting and governance structure and standing agenda items, which include 'Item 9 – Business Continuity, Item 11- FOI and SAR, Item 12 - ICT/ Cyber-Resilience' and 'Item 13 – Data Protection incl. Records Management' for the quarterly Strategic Governance Meeting, and 'Item 4 Policies and Procedures' for the SBC monthly Management Team Meeting, are detailed in the <i>Scheme of Governance and Risk Management Handbook</i> (version 2 dated May 2023). A link has been provided and this document is published on the authority's website, Information Scottish Biometrics Commissioner.</p> <p>A link has also been provided to the published minutes of the Monthly Management Team Meeting and Quarterly Strategic Governance Meetings.</p> <p>The SBC note the intention to include certain records management provisions, information security and business continuity, in future internal audit activities (see elements 8 and 10). This is commended by the Keeper, who can be updated on when this is in place through the PUR mechanism.</p> <p>The <i>RMP</i> (page 20) explains that any changes and updates to the <i>RMP</i> will be approved by the Commissioner (named at element 1) and presented to the Advisory Audit Board. The SBC commit to ensuring the Keeper is informed of changes and</p>
--	--	--	--

			<p>updates.</p> <p>The SBC manage their public records on the systems of the SG; therefore, the Keeper must be confident that the authority has processes in place to communicate updates and changes between authorities. The SBC will be notified of changes and updates to the eRDMs through liaison with an assigned iTECS Customer Relationship Manager and general communications from iTECS (<i>RMP</i> page 20). The role of the Customer Relationship Manager is outlined in the <i>iTECS ICT SCOTS Connect services Terms of Supply</i> (page 9). The Keeper has previously agreed the review processes implemented by the SG.</p> <p>As well as the assurance of an overall <i>RMP</i> review, most individual elements have an annual review commitment or commitment to “ongoing monitoring and review” and details of who should conduct that review. This is noted in an ‘Assessment and Review’ section which forms part of each element of the <i>RMP</i>.</p> <p>Sections of the <i>Information Governance Handbook</i> also contain notes of when reviews will take place, for example the <i>Clear Desk and Screen Policy</i> (page 2), “This policy will be continually monitored and will be subject to a regular review which will take place one year from the date of issue and annually thereafter. The review will be carried out by the Corporate Services Manager.” And “The eRDM archiving policy will be reviewed by Scottish Government while the SBC will review their website content, the Records Management Plan and Policy and the File Plan annually or as legislation and/or policy change.” (page 14)</p> <p>The Keeper agrees that the Scottish Biometrics Commissioner have made a firm commitment to review their <i>RMP</i> as required by the Act and have explained who will conduct this review and by what methodology. The Keeper further agrees that supporting policy and guidance documents have appropriate review periods allocated.</p>
--	--	--	--

<p>14. Shared Information</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects a Scottish public authority to ensure that information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.</p> <p>The Scottish Biometrics Commissioner state in their <i>Records Management Policy (Information Governance Handbook page 6)</i> that one of the benefits of implementing records management systems and processes is improved information sharing and the provision of quick and easy access to the right information at the right time.</p> <p>The <i>RMP</i> explains the SBC share information with other authorities and manage these arrangements through the use of data sharing agreements.</p> <p>An <i>Information Sharing Policy</i> forms part of the <i>Information Governance Handbook</i>. It states “We need to share information with others to do the jobs under the powers and duties the Scottish Parliament gave us.” And it explains the several ways in which the SBC may share information and the authorities it may share information with.</p> <p>The <i>Information Sharing Policy</i> refers to specific sections of the Scottish Biometrics Commissioner Act 2020 which relate to information sharing. It also outlines the procedures and guidance in place to manage this.</p> <p>A copy of the <i>Data Sharing Agreement</i> between the SBC and the Police Scotland for “the necessary sharing of personal data” (dated December 2022) has been provided. This includes section on information assurance and security, information management, and retention and disposal.</p> <p>As noted at element 9, the SBC have policies and procedures in place to ensure</p>
-------------------------------	-----------------	-----------------	---

			<p>compliance with data protection legislation.</p> <p>The <i>RMP</i> also explains how the SBC routinely publish information online through their <i>Publication Scheme</i>. A link to this document on the SCB website has been provided Information Scottish Biometrics Commissioner.</p> <p>The Keeper can agree that the Scottish Biometrics Commissioner properly considers records governance when undertaking information sharing programmes.</p>
<p>15. Public records created or held by third parties</p>	<p>N/A</p>	<p>N/A</p>	<p>The 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).</p> <p>The <i>RMP</i> (page 22) explains that a shared services agreement is in place for certain services which are provided by the SPSO, but is clear that "...no functions of the Scottish Biometrics Commissioner's office is contracted out to third parties..."</p> <p>The <i>Statement from the Commissioner</i>, provided as evidence, confirms this, "I can also confirm that no legal functions assigned to me by virtue of the Scottish Biometrics Commissioner Act 2020 are otherwise contracted out to any third party. This position will not change during my tenure as Commissioner."</p> <p>The Keeper accepts that this element is not applicable to the Scottish Biometrics Commissioner, however, should this situation change the Keeper expects to be notified.</p>

General Notes on submission:

This assessment is on the Records Management Plan of the Scottish Biometrics Commissioner submitted to the Keeper on 28 February 2023. The Records Management Plan submitted was dated February 2023 and is version 1.0. The Keeper acknowledges that an updated Records Management Plan (version 2.0, dated July 2023), which incorporated minor changes, was submitted during the assessment process. The author is Cheryl Glen, Corporate Services Manager, named at element 2, and it was reviewed by the Commissioner Dr Brian Plastow, named at element 1.

A supporting statement from the Commissioner, dated 3 February 2023, has been provided. It notes “I write to provide a written policy note record in support of the forthcoming formal submission of our RMP to The Keeper of Records.” It also supports elements 2, 12 and 15 of the RMP. The Commissioner commits to “providing and supporting access to training and development around records management to all staff, and on an ongoing basis.”

The *Records Management Policy within SBC Information Governance Handbook* includes the following statement, “Records are a vital information asset and a valuable resource for the organisation's decision-making processes, policy creation and operations and must be managed effectively from the point of their creation until their ultimate disposal.”

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 Biometrics Commissioner. Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development by the Scottish Biometrics Commissioner are as follows:

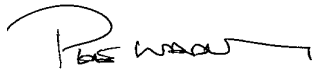
Element 6. Destruction Arrangements

7. Keeper's Determination

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

- The Keeper recommends that the Scottish Biometrics 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 the Scottish Biometrics Commissioner. In agreeing this RMP, the Keeper expects the Scottish Biometrics Commissioner to fully implement the agreed RMP and meet its obligations under the Act.



.....

Laura Mitchell
Deputy Keeper of the Records of Scotland