

Public Records (Scotland) Act 2011

Police Scotland

The Keeper of the Records of Scotland

9th August 2022

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	7-51
6. Keeper's Summary	52
7. Keeper's Determination	53
8. Keeper's Endorsement	54

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 Police Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 28 May 2021.

The assessment considered whether the RMP of Police Scotland was developed with proper regard to the 15 elements of the Keeper's statutory Model Records Management Plan (the Model Plan) under section 8(3) of the Act, and whether in this respect it complies with it and the specific requirements of the Act.

The outcome of the assessment and the Keeper's decision on whether the RMP of Police Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

Police Scotland was established on 1 April 2013 and is responsible for policing across the whole of Scotland, some 28,168 square miles, covering a third of the United Kingdom's landmass with a unique range of urban, rural, island and remote communities

It is the second largest force in the UK after the Metropolitan Police with a workforce of 23,000 officers and staff working together for the people of Scotland.

Police Scotland's purpose is to improve the safety and wellbeing of people, places and communities in Scotland, focusing on keeping people safe in line with our values of integrity, fairness and respect.

The service is led by Chief Constable Iain Livingstone QPM, supported by a command team of three Deputy Chief Constables, a Deputy Chief Officer, Assistant Chief Constables and Directors.

There are 13 local policing divisions, each headed by a Chief Superintendent who ensures that local policing in each area is responsive, accountable and tailored to meet local needs. Each division encompasses response officers, community officers, local crime investigation, public protection and local intelligence.

The headquarters of Police Scotland is based at the Scottish Police College, Tulliallan, in Fife.

[Police Scotland - Police Scotland](#)

4. Keeper's Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether Police Scotland's RMP was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

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

5. Model Plan Elements: Checklist

Element	Present	Evidence	Notes
1. Senior Officer	G	G	<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>Police Scotland have identified Alan Speirs, Assistant Chief Constable Professionalism and Assurance, as holding overall responsibility for records management in the organisation.</p> <p>The identification of the Assistant Chief Constable (ACC) Professionalism and Assurance to this role is evidenced by a <i>Letter from the Accountable Executive Officer</i> (dated 27 May 2021) and <i>Information Governance Standard Operating Procedure (SOP)</i>, version 2.0, dated August 2020 (section 5). His approval of the Records Management Plan (<i>RMP</i>) is confirmed in the <i>Letter from the Accountable Executive Officer</i>.</p> <p>The ACC Professionalism and Assurance acts as the Senior Information Risk Officer (SIRO) and the Accountable Executive Officer. These roles are confirmed and the responsibilities outlined in the <i>Information Governance SOP</i> (sections 5 & 6) and <i>Management of Records SOP</i> (version 3.0 dated January 2021) (section 2).</p> <p>As SIRO, the ACC Professionalism and Assurance chairs the Data Governance Board (DGB). The <i>Data Governance Board Terms of Reference</i> (version 1 dated May 2020), which has been supplied, outlines the purpose and remit of the DGB</p>

			<p>and specifically mentions records management and oversight of legislation, including the Public Records (Scotland) Act.</p> <p>The role is supported by supported by Strategic Information Asset Owners (SIAOs), who are members of the Force Executive and can report through the DGB.</p> <p>The ACC Professionalism and Assurance has undertaken Strategic Information Asset Owner (SIAO) training, required for all SIAOs, which is delivered by the Records Manager (see element 2), Information Security Manager and Information Manager (Assurance).</p> <p>The ACC Professionalism and Assurance also chairs the Data Retention Oversight Group (DROG) (see elements 5).</p> <p>It is clear from the above that the Assistant Chief Constable Professionalism and Assurance is closely aware of the records management provision in Police Scotland.</p> <p>The Keeper of the Records of Scotland (the Keeper) agrees that Police Scotland have identified an appropriate individual to this role as required by the Act.</p>
2. Records Manager	G	G	<p>The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and that staff member has appropriate corporate responsibility, access to resources and skills.</p> <p>While Police Scotland have identified the post of Records Manager as holding operational responsibility for records management and implementing the RMP, it has been confirmed separately that this post will be vacant from mid-July 2022. Police Scotland have provided the following assurance, “Until such a time as this vacancy is filled, Police Scotland’s named individual under</p>

			<p>Element 2 will be Alice Stewart, Information Manager (Assurance). Following the successful appointment of a new Records Manager, the Keeper will be updated.”</p> <p>The identification of the Records Manager to this role is supported by a <i>Letter from the Accountable Executive Officer, Alan Speirs</i> (see element 1) and the <i>Records Management Policy</i> (version 1.01 dated 2014).</p> <p>The Records Manager post is supported by a Records Officer and an Information Assistant. The Records Manager is further assisted by Information Assurance Officers, who are part of the wider Information Assurance section which includes the Records Management Team. Since submission it has been confirmed separately that a number of personnel changes have taken place. These include the Records Officer named in the <i>RMP</i> and the creation of several additional posts.</p> <p><i>Job descriptions</i> for all the above mentioned roles have been provided. These further support the identification of the Records Manager under this element.</p> <p>The <i>Information Governance SOP</i> (section 6) and <i>Management of Records SOP</i> (section 2) outline the roles and responsibilities of the Records Manager, including briefing the Accountable Executive Officer (AEO) (named at element 1) on appointment.</p> <p>The <i>Management of Records SOP</i> (section 2) lists among the roles and responsibilities for the Records Manger, “Provides regular updates to the Accountable Executive Officer on records management arrangements”. It has been confirmed separately that the Records Manager has direct access to the AEO and reports directly to the AEO to provide updates on PRSA on a one-to-one basis as necessary.</p>
--	--	--	--

			<p>The Records Manger is a member of the Data Retention Oversight Group (DROG) (see General Comments) and it has been confirmed separately since submission that the role of Records Manager is now also a member of the Data Governance Board (DGB) (see General Comments). Prior to being added as a member, the Records Manager’s engagement with the DGB was through the submission of reports. A report submitted in May 2022 recommended that further updates on PRSA are part of the substantive agenda items. The Information Assurance Manager, to whom the Records Manager directly reports, is also part of the DGB. Several staff members attend both the DGB and the DROG, including the Data Protection Officer and Head of Information Management and the DROG reports to the DGB.</p> <p>The Records Manager is responsible for the governance, maintenance and development of the Information Asset Register (IAR) and the creation and maintenance of the IAR operating manual (<i>Information Governance SOP</i> section 6).</p> <p>The Records Manger and Records Management Team develop and deliver records management training, including formal training to SIAOs on their roles as information asset owners, and training on the use of the records management systems of external storage suppliers.</p> <p>The Keeper agrees that Police Scotland have identified an appropriate individual to this role as required by the Act. However, the Keeper requires that he is updated once the vacant Records Manager post is filled.</p>
3. Policy	G	G	<p>The Act requires an authority to have an appropriate policy statement on records management.</p> <p>Police Scotland have a <i>Records Management Policy</i>, version 2.00, dated May 2022.</p>

			<p>The Keeper has been provided with a copy.</p> <p>Police Scotland state they “will ensure it meets its obligations under the Public Records (Scotland) Act 2011 and other relevant legislation, including data protection and freedom of information legislation.” And that this will be done by “adhering to the principles of good records management as outlined in its own Records Management Plan (RMP).” (<i>Records Management Policy</i>)</p> <p>A previous version of the <i>Records Management Policy</i> (version 1.01 dated 2014) is publically available at Police Scotland Policies - Police Scotland. It has been confirmed separately that this is due to an internal decision “not to publish further PDF documents to the website until a process is in place to ensure PDF and other documents are created in a manner compliant with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018. This issue is recorded on the corporate risk register, however a date for achieving compliance and resumed publication is at present unknown.”</p> <p>The updated <i>Records Management Policy</i>, along with all Police Scotland Standard Operating Procedures (SOPs) and guidance are available on the staff intranet. Screenshots have been provided showing this.</p> <p>The <i>Records Management Policy</i> is supported by the <i>Management of Records SOP</i> (version 3.0 dated January 2021) and the <i>Record Retention SOP</i> (version 4.00 dated November 2020). These SOPs are published on the Police Scotland website, Standard Operating Procedures - Police Scotland.</p> <p>The <i>Management of Records SOP</i> (section 1) “outlines requirements that must be followed by all PS Officers and Staff for the management of all electronic and hardcopy records created or received by Police Scotland, including those stored with external storage suppliers.” It states Police Scotland recognise that “Records</p>
--	--	--	--

			<p>are a vital asset... in maintaining operational integrity and public trust, but they can also present significant financial and reputational risk where not managed robustly.”</p> <p>The Keeper notes the change to guidance documents, with some information now removed from SOPs and included in Divisional Guidance, specifically email management, file and folder naming conventions and offsite storage usage. The Keeper acknowledges the highlighted resulting risks from the differing processes for creation, approval, management and review of these documents. Divisional Guidance (for example <i>Management of Records Divisional Guidance</i> and <i>Business Continuity Management Divisional Guidance</i>) is the responsibility of the creating division even when it is applicable to all of Police Scotland. Divisional Guidance “does not form part of the formal Police Scotland record set, nor is it subject to the formal version control, governance and consultation outlined above.”(<i>RMP</i> page 8) A copy of <i>Governance of the Police Scotland Record Set</i> (version 1.00 dated March 2020) has been provided. The Keeper also notes the commitment to address this risk, as outlined in the development plan (<i>RMP</i> page 9), and expects to be updated on progress.</p> <p>The Keeper agrees that the <i>RMP</i> supports the objectives of the <i>Records Management Policy</i> and supporting <i>SOPs</i>.</p> <p>The Keeper agrees Police Scotland have a formal records management policy statement as required by the Act.</p>
4. Business Classification	A	G	<p>The Keeper expects that the public records of an authority are known and are identified within a structure.</p> <p>Section 5 of the <i>Management of Records SOP</i> explains business classification and notes that records are “mapped to the operational / business functions carried out by PS on a daily basis.” and “Records are defined by the activity they relate to,</p>

			<p>regardless of whether they are electronic or hardcopy.” (<i>Management of Records SOP</i> page 3)</p> <p>Police Scotland operate a hybrid system: Public records are held digitally on SharePoint, network shared drives, personal drives and email, which the <i>RMP</i> refers to as unstructured electronic records; and in line-of-business systems, which the <i>RMP</i> refers to as structured electronic records (<i>RMP</i> page 33). There are also public records held in hard-copy format onsite in Police Scotland premises and offsite by a third party storage supplier.</p> <p><u>Digital - SharePoint, shared/personal drives and Outlook:</u></p> <p>A single national network is in place (SPnet) which replaced nine legacy networks. A national file plan and business area file plans have been created. A national local file plan was implemented to ensure consistency across all divisions. The <i>Spotlight on V Division Presentation to the DROG</i>, which has been provided, contains a series of screenshots showing a file plan in shared drives. The Records Management Team manage this file structure and control user access. This is done through User Access Management (UAM) processes. Guidance has also been produced to support these measures (<i>UAM Guidance</i>) and a copy has been provided. A <i>SP File Plan</i> records a list of secure folders and is accessible to UAM authorisers. The <i>SP File Plan</i> will continue to be developed and will assist with ongoing work around the IAR. A screenshot of <i>SP File Plan for UAM Authoriser</i> has been provided.</p> <p>Guidance on the management of electronic records is included in the <i>Management of Records SOP</i> (section 7). Any records in Outlook are saved to the relevant shared drives area. Guidance on this process and email management is outlined in the <i>Management of Records Divisional Guidance</i> (section 2).</p> <p>Digital Line-of-business:</p>
--	--	--	---

			<p>Police Scotland have a considerable number line-of-business systems in which public records are created, managed and stored. The Keeper can agree that these line-of-business systems are likely to allow the appropriate management of records within a structure as required. Work is ongoing through the ICT Systems List to identify systems with limited records management functionality and the DROG is progressing work to address issues around retention and disposal (see elements 5, 6, 9 and 11).</p> <p><u>Hard copy onsite:</u> Hard-copy records are stored onsite in Police Scotland premises. Storage arrangements for hardcopy records were rationalised and work is ongoing to ensure all records are identified, listed and added to the Information Asset Register (IAR). This is being undertaken by the DROG through the use of Highlight Reports. These require business areas to provide regular updates on progress (see element 11). Indexes listing hardcopy records stored onsite are saved in the relevant area of the shared drives or ICT system (<i>Management of Records SOP</i> section 6).</p> <p><u>Hard copy offsite:</u> After a rationalisation of storage arrangements there is a single national contract in place for offsite records storage with a third party provider. An online portal allows each business area to have oversight of records stored. (<i>RMP</i> page 17). The Records Management Team oversee this and train staff who are given access to the online system to send/retrieve records. In addition, an index of records sent to offsite storage is retained by the relevant business area. The <i>Management of Records Divisional Guidance</i> (section 4) provides staff with instructions on the processes for offsite records storage.</p> <p>Police Scotland have in place “a number of interlinked mechanisms for classifying records: a Business Classification Scheme (BCS) that outlines the functions and activities performed by PS; a national file plan for shared drives; and a national</p>
--	--	--	--

			<p>naming convention for shared business mailboxes and other communication platforms. All mechanisms for creating and storing records, including but not limited to, shared drive folders, shared business mailboxes, SharePoint sites and accounts with external storage suppliers, will be structured according to these classifications, with all amendments subject to approval from Records Management.” (<i>Management of Records SOP</i> section 5)</p> <p>Police Scotland have a national file plan, as noted above, a Subject Area Model (SAM) and Information Asset Register (IAR).</p> <p>The SAM has been developed by the Records Manager and Data Governance lead and acts of the authority’s business classification scheme. It incorporates elements of a draft BCS and is intended to eventually replace it. The SAM “presents an up-to-date business classification of Police Scotland functions (i.e. subject areas).” (<i>RMP</i> page 12). Arrangement by function is currently considered best practice. A copy of the SAM has been provided.</p> <p>The <i>Letter from the Accountable Executive Officer</i> confirms the use of the SAM “as the top level, functional classification scheme for our data, information and records...” and that “further development work is required before it reaches the necessary maturity level.” The Keeper acknowledges that further work is identified to develop the SAM and expects to be updated on progress. This can be done through the Progress Update Review (PUR) reporting mechanism, Progress Update Reviews National Records of Scotland (nrscotland.gov.uk).</p> <p>An IAR was developed and implemented as part of a wider Data Protection Reform Project. It was populated initially through information provided by business areas. It was then aligned to a previously developed draft BCS. This allows information assets to be viewed by function. The IAR is used as Police Scotland’s record of</p>
--	--	--	--

			<p>processing (see element 9). The IAR includes records in all formats. The RMP explains work undertaken, the planned development and ongoing work on the IAR, including the mapping of IAR entries against the SAM. An extract of the IAR has been provided. The Keeper wishes to be updated as this work progresses.</p> <p>Police Scotland are in the process of implementing an electronic records and document management system (EDRMS) in one business area. The Records Management Team are involved in this work and Police Scotland commit to updating the Keeper on progress and any plans to expand implementation. A further update has been provided separately since submission, “The EDRMS implementation within our People and Development department is nearing completion... Processes have been put in place to ensure that the full lifecycle of a personnel record is only electronically held. The implementation project is nearly complete with only final data quality checks left to be finished. Due to the current status, a more substantive update will be forthcoming under the PUR Process once the system has been fully operational for a longer period of time.”</p> <p>Since submission, an update has been provided separately on the implementation of M365 and the use of SharePoint, “With regard to the implementation of M365 within Police Scotland, the initial scoping of pre-requisites is still ongoing. This has been a lengthy process due to the additional security requirements placed on Police Scotland as a member of the UK Community of Policing... Police Scotland is nearly complete with its roll-out of MS Teams with over 22,000 out of 23,000 users on the platform. The Digital Division is also currently reviewing the list of M365 apps to determine what will be included for users in the initial implementation.” The Keeper looks forward to future updates on progress.</p> <p>The Keeper acknowledges and commends the work of the Records Management Team to develop a single national file plan, implement and develop guidance around</p>
--	--	--	--

			<p>User Access Management and the ongoing work developing the IAR and SAM.</p> <p>The Keeper notes the planned work outlined under the development plan, including the Digital Drives Data Programme.</p> <p>Police Scotland have identified that further work is required to developed the SAM in conjunction with the IAR and that an EDRMS is being introduced to certain business areas. While this work is progressing the Keeper can agree this element on an ‘improvement model’ basis and on the condition that he is updated on progress.</p>
5. Retention schedule	A	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>Police Scotland have a <i>Record Retention SOP</i> (version 4.00 dated November 2020). A link to which has been provided and is also published online, Standard Operating Procedures - Police Scotland. This document lists staff responsibilities, provides guidance to staff and allocates retention periods to all Police Scotland records regardless of format. The retention schedules are arranged by function. An example entry includes:</p> <p><i>Ref.</i> OSS-013 <i>Function Description</i> Register of dog and handlers trained <i>Trigger</i> Current year <i>Retention</i> Until business/operational requirements have ceased <i>Action</i> Offer to Archive <i>Examples of Records</i> <i>Notes</i></p> <p>The <i>Record Retention SOP</i> (section 4) contains staff guidance on destruction,</p>

			<p>review and transfer to archive. It also contains a section on moratoriums on destruction (section 6). Strategic and Tactical IAOs are responsible for ensuring records retention schedules are implemented for records within their remit. Strategic Information Asset Owners (SIAOs) are responsible for managing the disposal of information assets and receive training on records retention.</p> <p>The Keeper acknowledges significant work has been undertaken to revise this document resulting in the first unified Police Scotland <i>Record Retention SOP</i>. He also notes the work carried out in response to areas highlighted for improvement in an internal audit. Police Scotland commit to further revisions to fully address issues around clarity of instruction, for example around transfer to archives, and an explanation of retention periods. The Keeper can be updated as this work progresses through the PUR process.</p> <p>Updates in response to legislative changes indicate recognition that retention schedules will be subject to regular changes, including to meet business needs. This recognition along with consultation with business areas in developing retention decisions is commended. This is further supported by the development of a <i>Record Retention Changes Framework document</i>, a copy of which has been supplied. This provides business areas with guidance when changes to retention periods are required. Changes are monitored internally by the Records Management Team using a tracker system. Changes to the <i>Record Retention SOP</i> go through the Policy Support function for review. However, the Keeper notes that changes to the <i>Record Retention SOP</i> can take several months to go through the review process for approval and subsequent implementation.</p> <p>The <i>Record Retention SOP</i> explains the use of a Records Destruction Authorisation form, which also records when a decision is taken to retain records beyond their allocated retention period. The use of this form is commended by the Keeper. This form is then sent to the Records Management Team. A <i>Sample Record Destruction</i></p>
--	--	--	---

			<p><i>Authorisation Form</i> has been submitted. Use of the <i>Form</i> is evidenced in the submitted <i>DROG Overview Report April 2022</i>. Since submission Police Scotland have provided an update on the use of the <i>Form</i>, “each Division has been tasked via the Data Retention Oversight Group (DROG) to progress on-site hard copy record destruction and to use the form to capture the destruction and authorisation. In preparation for the last DROG meeting in April 2022 an analysis was undertaken of use of this form over the past year and this was summarised and presented to the membership in a chart found on page 5 of the evidence submitted. This chart shows an ongoing inconsistency in use of the form, but a general trend of increasing use over time culminating in a large spike in use at the beginning of 2022. This indicates growing effectiveness of the governance that the DROG seeks to bring to this area through the formal tasking of this work via divisional leads and indicates increased adoption of the destruction process at the intended end of ‘current year’ retention cycle.” The Keeper welcomes this update and commends Police Scotland on their work around the use of the destruction form.</p> <p>Staff guidance on the destruction of records is outlined in the <i>Management of Records SOP</i> (section 9) and should be carried out in line with the <i>Information Security SOP (Records Retention SOP</i> page 4). Data protection legislation is considered in the level of information (series or file) retained in the record of destruction and guidance is outlined in the <i>Management of Records SOP</i>.</p> <p>Records retention provision is in place for Data Protection Impact Assessments (DPIAs) and Information Sharing Agreements (ISAs). Copies of a <i>DPIA</i> and <i>Information Sharing Agreement template (general processing)</i> have been submitted. This focus on records retention promotes early engagement with local business areas when new records types are created or new technologies are introduced. The Keeper commends this approach.</p> <p>Police Scotland have a Data Retention Oversight Group (DROG) chaired by the</p>
--	--	--	---

			<p>ACC. (see element 1 and General Comments below). The focus of the DROG is to address the over-retention of records in all formats and systems. The <i>DROG Terms of Reference</i> has been submitted. Highlight reports are submitted at bi-monthly meetings from senior managers in each business area to provide updates on progress. A <i>DROG Report V Division</i> and <i>DROG Overview Report April 2022</i> (noted above) have been provided. Divisional highlight reports require divisions to provide updates through a series of questions on aspects of availability and data retention for hardcopy (onsite and offsite), unstructured and structured records. Records retention features in local risk registers and there are also local data retention sub-groups. Sub-groups carry out work required by the DROG and feed into reports submitted to it. A copy of <i>OSD Data Retention Review Group ToR</i> has been supplied.</p> <p>Over-retention of data is on Police Scotland’s organisational risk register, “due to inconsistent or even complete lack of adherence to the retention schedules and instances where weeding capability within systems is simply non-existent.” (RMP page 17). An <i>Organisational Risk Register Extract – Retention</i> has been supplied. The over-retention of data in three formats is highlighted by Police Scotland, hardcopy, unstructured electronic and structured electronic data. The <i>Letter from the Accountable Executive Officer</i> highlights Police Scotland’s commitment to managing over-retention through the Force Weeding Project. The acknowledgment of issues around the current ability to ensure retention decisions are implemented is noted by the Keeper.</p> <p>The Keeper acknowledges and commends the substantial work already undertaken and continuing to be carried out to mitigate this risk. This work includes weeding (hardcopy and electronic records), reporting to the DROG on shared drive and mailbox use, and review of management of hardcopy records after moving to a single offsite records storage solution. The <i>RMP</i> explains the progress made and planned development work. Evidence has been provided showing how this work in</p>
--	--	--	---

			<p>communicated to staff through intranet news stories.</p> <p>The size and complexity of Police Scotland means there are numerous line-of-business systems in use, some of which have no capacity for records retention allocation, thereby resulting in the over-retention of data. The Keeper notes this issue and acknowledges that addressing it will take time. An outline of several measure being taken has been provided, including the Core Operational Solutions (COS) programme. This will replace some of the legacy systems and ensure records retention is considered at the outset of new systems (RMP page 18). The Keeper will be interested in how this work progresses and can be updated through the PUR process.</p> <p>A single national contract for offsite records storage is in place. All hardcopy records sent to offsite storage must have an allocated retention date. An online portal allows each business area to oversee records stored and access reports to identify and review records due for disposal and take the appropriate action. Training is provided by the Records Management Team to staff accessing the portal (RMP page 17).</p> <p>The Data Drive Programme “aims to ensure that data is captured, managed, protected and accessible to the benefit of Police Scotland and its partners.” (RMP page 12) As part of this work there are planned projects which aim “to bring in technology that will support the automatic classification of structured and unstructured content to aid with retention and weeding decisions.” (RMP page 12) The programme “will deliver several projects that will aid automatic classification of unstructured information in order to allow weeding and retention policy to be applied. This will be key in the Force’s approach to managing retention of the significant volumes of data that it holds.” (RMP page 19) The Keeper welcomes this approach of adopting new technologies to manage retention and looks forward to being updated on progress as this programme progresses.</p>
--	--	--	---

			<p>Police Scotland have a <i>Records Retention SOP</i>, which outlines retention periods for all public records. The allocation of these retention periods and the resulting retention or disposition is ongoing as work around mitigating over-retention and developing in-built retention functionality in line-of-business systems continues. Therefore the Keeper can agree this element on an ‘improvement model’ basis with the condition he is kept updated. The Keeper acknowledges the evident progress already made and the clear commitment to continuing to address these areas.</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 secure destruction of Police Scotland public records is managed under the <i>Record Retention SOP</i> and <i>Information Security SOP</i> (version 4.00 dated September 2018). These documents, along with the <i>Information Security Handbook Divisional Guidance</i> (version 4.00 dated January 2021) and <i>Management of Records SOP</i> provide guidance to staff.</p> <p>The <i>RMP</i> (page 21) states Police Scotland will “conform to Her Majesty’s Government Information Assurance Standard 5; Secure Sanitation for the destruction of paper assets and electronic information, as well as ensuring that equipment used conforms to that within the Catalogue of Security Equipment issued by the Centre for Protection of National Infrastructure (CPNI).”</p> <p>It is the responsibility of Strategic Information Asset Owners (SIAOs) to oversee “the disposal of information assets as stipulated in the Information Governance SOP.” (<i>RMP</i> page 16).</p> <p>Police Scotland have the following processes in place for ensuring the secure and irretrievable destruction of public records:</p>

			<p><u>Digital - SharePoint, shared drives and Outlook:</u> Records destruction for shared drives is done manually through the use of retention periods specified in the <i>Records Retention SOP</i>. Reports on shared drives, including folder age, are collated by the Records Management Team and reported to the DROG. Ongoing identification and weeding of records due for destruction is reported to the DROG through the use of Divisional Highlight Reports. The <i>Management of Records SOP</i> (page 8) notes “where records are automatically destroyed by an electronic system, that system should have the capability to evidence weeding rules in place at a given time.” SharePoint has built-in automated deletion. As noted above, a <i>Records Destruction Authorisation Form</i> is in use. This form “provides a format for recording record series and / or files that have been destroyed (electronic or paper)...” (<i>Records Retention SOP</i> page 3). See comments on the use of this form under element 5.</p> <p><u>Digital – line-of-business systems:</u> The <i>Management of Records SOP</i> (page 8) notes that some electronic systems have automatic records deletion functionality which will be able to provide evidence of destruction. Where this process is not automated, the ongoing identification and weeding of records due for destruction is reported to the DROG through the use of Divisional Highlight Reports. In some cases line-of-business systems are unable to irretrievably destroy records (RMP page 22).</p> <p><u>Digital Backups:</u> Minimum retention periods for backups on various systems are listed in the <i>ICT Backup Policy</i> (page 3), e.g. “for SQL a monthly point-in-time backup on production systems is kept for 12 months. Backup schedules and retention policies may be altered if there are special considerations for an application e.g. Year-End Finance requirements or major application upgrades.”</p>
--	--	--	---

			<p><u>Digital hardware:</u> Electronic media is securely destroyed through a CPNI approved contractor to HMG IA Standard 5. A process is in place for Police Scotland staff to supervise destruction. An inventory of destruction is maintained and the contractor provides destruction certificates. Samples of each have been provided as evidence. Section 13 of <i>Information Security Handbook Divisional Guidance</i> explains the processes in place for the secure destruction and disposal of ‘electronic media storage devices’.</p> <p><u>Hard copy onsite</u> – A third party company provides secure shredding services to all onsite locations under a single national contract. A copy of a <i>Shred-it destruction certificate</i> has been provided. Secure, lockable confidential waste cabinets are in place in offices with the contents routinely disposed of by the service provider. Where required, an ad hoc service is also provided and is available on request for larger volumes. Secure destruction is supervised by Police Scotland staff and destruction certificates are supplied by the service provider. A sample onsite destruction certificate has been provided. Any local onsite shredders must meet CPNI standards. Section 13 of <i>Information Security Handbook Divisional Guidance</i> explains the processes in place for the secure destruction and disposal of hard copy records, this includes “paper assets” and “soft copy assets i.e. CD-ROM and DVD.” Under home working arrangements staff are advised all hard copy records must be returned to offices to be securely destroyed (<i>Home Working – Information Security</i> page 6).</p> <p><u>Hard copy offsite</u> – All offsite records storage is managed by a single provider. All boxes sent to offsite storage must have an allocated retention period for review or destruction. The <i>RMP</i> states there are secure destruction processes in place and destruction certificates are produced. A sample destruction certificate and corresponding screenshot of the web portal used to manage boxes of records showing the ‘destroyed’ status’ have been provided.</p>
--	--	--	--

			<p>As noted in element 5, and reiterated at <i>RMP</i> (pages 21-22) “work is being progressed through the DROG to address inconsistent weeding and retention practice across hard-copy, structured and unstructured data. This remains a point for development and therefore destruction is not systematic and in areas the force is failing to destroy personal information in accordance with data protection legislation, particularly in relation to legacy systems.” The Data Drives Digital Programme “aims to address this issue for structured and unstructured data sets through the automatic classification and remediation, including deletion, of data, with a particular focus on remediating data protection risk.” (<i>RMP</i> page 22).</p> <p>The Keeper can agree this element on an ‘improvement model’ basis as a gap in provision has been identified (secure, irretrievable destruction of electronic records is not being carried out systematically across all locations (shared drives, line-of-business systems). Work is underway to address this gap in provision and the Keeper’s agreement is conditional on being updated on progress.</p>
7. Archiving and Transfer	A	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>Police Scotland recognise that certain records will be retained for permanent preservation and this is acknowledged in the <i>Management of Records SOP</i> (page 4) which states, “In the longer term, certain records are relied on to show the history of policing.”</p> <p>Police Scotland have provided an outline of the considerable work carried out around the management of and deposit arrangements for records of predecessor Police Forces. This relates to records created prior to 1 April 2013, which are held in</p>

			<p>various archival repositories, and will be managed by a standard deposit agreement which will be put in place with each individual repository. Work is ongoing concerning confirmation of ownership of these records, including those which are held by Police Scotland, and to finalise a deposit agreement. The issue of ownership is complex and the work being undertaken to ensure this is appropriately reflected in the finalised deposit agreement is commended by the Keeper. A copy of <i>SPA Property Transfer Scheme 2013</i> has been provided, as has a copy of the draft <i>PSoS Deposit Agreement</i>. The Keeper looks forward to being updated as this work progresses.</p> <p>The <i>Record Retention SOP</i> lists the identification of records with enduring historical value as an objective. As a result of an internal audit, work has been carried out to provide additional guidance explaining the action 'transfer to archive'. Further work to provide clarity of guidance when records are identified for archival transfer is noted under the development plan section. The ongoing Force Weeding Project is also identifying records for permanent preservation.</p> <p>Records to be transferred to archival storage are retained onsite. The <i>Management of Records Divisional Guidance</i> (page 17) is clear that records identified for permanent retention are not considered suitable for offsite storage. The Records Management Team will have oversight over any records transferred to an archive. (<i>Records Retention SOP</i> page 5). The <i>Management of Records SOP</i> (section 10) provides staff guidance on archiving arrangements.</p> <p>The Records Management Team have also carried out engagement work to ensure Police Scotland Museums have a clear understanding of the requirements around public records.</p> <p>Police Scotland have selected National Records of Scotland (NRS) as the repository for records (created from 1 April 2013) identified for permanent preservation. NRS is</p>
--	--	--	--

			<p>an accredited archive National Records of Scotland receives Archive Accreditation Award National Records of Scotland (nrscotland.gov.uk) and fully adheres to the Keeper's <i>Supplementary Guidance on Proper Arrangements for Archiving Public Records</i>: https://www.nrscotland.gov.uk/files//record-keeping/public-records-act/supplementary-guidance-on-proper-arrangements-for-archiving-public-records.pdf. Police Scotland commit to progressing work towards securing a deposit agreement with NRS once work is completed to finalise the deposit agreement for records of predecessor police forces. Progressing this is noted in the development plan sections for both elements 5 and 7. While the Keeper understands work on deposit arrangements for legacy force records has been a priority, he would encourage Police Scotland to actively pursue an agreement with NRS. Since submission it has been confirmed separately that initial contact has been made with the NRS Client Manager and that a meeting is yet to be arranged.</p> <p>The Keeper can agree this element on an 'improvement model' basis as a gap in provision has been identified (Police Scotland do not yet have a formal deposit agreement in place with NRS; and work is ongoing to finalise a deposit agreement that will manage the records of legacy forces retained for permanent preservation). Police Scotland have committed to progressing these areas and to updating the Keeper.</p>
8. Information Security	A	G	<p>The Act requires that public records are held in accordance with information security compliance requirements.</p> <p>The <i>RMP</i> outlines the technical, physical, procedural and behavioural controls in place to ensure information security. Section 11 of the <i>Management of Records SOP</i> states "All records must be classified, handled stored and destroyed in line with the Information Security SOP."</p>

			<p>Police Scotland have an <i>Information Security Policy</i> (version 1.01 dated February 2014), which is published on their public website. The <i>RMP</i> (page 25) states “Police Scotland’s Information Security Policy recognises the need to protect information assets in all formats from all threats whether internal, external, accidental or deliberate through a combination of personal, physical, procedural and technical controls.”</p> <p>The <i>Information Security Policy</i> is supported by an <i>Information Security SOP</i> which outlines the processes in place and is also published online. An <i>Information Security Handbook Divisional Guidance</i> and a <i>Home Working – Information Security</i> document provide additional guidance and address the security of both digital and hardcopy public records. Both of which have been provided as evidence. A screenshot has been provided showing staff can access these documents on the staff intranet site.</p> <p>Police Scotland is a member of the National Policing Community of Trust, members of which are expected to have security measures in place that meet “a baseline level of security as identified in Her Majesty’s Government (HMG) Security Policy Framework.” (<i>RMP</i> page 25).</p> <p>The <i>Information Security SOP</i> outlines roles and responsibilities and provides instruction on the measures in place. Sections include Computer Use Accounts (section 6); Acceptable Use (section 7); Information Classification, Marking and Handling (section 8); Clear Desk Policy and Overlooking (section 13) and Removal of Assets from Police Scotland Premises (section 16).</p> <p>The <i>Information Security Handbook Divisional Guidance</i> provides detailed guidance for staff “on how to apply the instructions within the SOP and must therefore be read in conjunction with the SOP.” Sections include: Acceptable Use Policy (section 3); Physical Security - Server/Computer Rooms (section 6); System Security (section</p>
--	--	--	---

			<p>7); Role-Based Access Controls (section 10); Handling and Communicating Classified Police Information - Technical Procedural and Behavioural Controls (section 11); and Mobile Devices and Remote Working (section 12).</p> <p>All Police Scotland systems are required to meet national policing accreditation standards and requirements of the Cabinet Office and Home Office Codes of Connection. A Lawful Business Monitoring system has been introduced. Information about which is included in the Acceptable Use Policy which all staff must agree to when logging on to Police Scotland systems. The Government Security Classification Scheme (GSC) is in use.</p> <p>Physical security measures are in place to control access to buildings. Risk assessments on the physical security for information held in police or partner body buildings are carried out by the Information Security Team.</p> <p>Physical and electronic information security measures are in place at third party offsite storage. The following documents have been provided to demonstrate the requirements met by the successful supplier in relation to information security, <i>Invitation To Tender (ITT) for the contract, associated Security Aspects Letter and part 1 of the Technical Response document.</i></p> <p>All staff (including contractors and agency staff) undergo a vetting process prior to employment, are required to complete an information security induction before gaining access to systems, and must sign an information security confidentiality declaration. Copies of the <i>Information Security and Confidentiality Declaration</i> and <i>SPA and Police Scotland Vetting Manual of Guidance</i> have been provided.</p> <p>Police Scotland have explained the measures in place to manage security incidents. The <i>Information Security SOP</i> and <i>Information Security Handbook Divisional Guidance</i> (section 14) outline responsibilities and contain staff guidance on</p>
--	--	--	--

			<p>identifying and reporting information security incidents. Processes are in place for managing serious or large scale information security breaches.</p> <p>The Data Governance Board (DGB) (see at element 1 and General Comments below) oversees information security compliance and reporting. The DGB is chaired by the SIRO, ACC Professionalism an Assurance (see element 1).</p> <p>Police Scotland have achieved Cyber Essentials Plus certification and a copy of the certificate has been supplied. This was renewed in July 2022.</p> <p>The <i>RMP</i> (page 32) notes the impact of network or ICT failures due to the increase in cyber security incidents will be form part of the Police Scotland business continuity exercise programme for 2021/22.</p> <p>Police Scotland is also working towards compliance with the Scottish Government Cyber Resilience Framework Cyber resilience: framework and self assessment tool - gov.scot (www.gov.scot) and carrying out work to develop offline backups. The Keeper commends this work and requests he is updated on progress.</p> <p>The Keeper acknowledges the highlighted “outstanding vulnerabilities” resulting from legacy hardware, legacy system support and the inherited ICT estate. He notes work is ongoing to actively monitor and mitigate these risks, and report to the DGB. Work is outlined under the development plan section and will be part of wider plans to deal with the issue of over retention and the incorporation of built-in retention and deletion functionality in systems (see elements 4, 5 and 6 above). As with other elements, the Keeper acknowledges Police Scotland’s commitment to provide annual updates through the PUR mechanism.</p>
--	--	--	---

			<p>The Keeper agrees that Police Scotland have procedures in place to appropriately ensure the security of their records as required by the Act. However, as gaps in provision have been acknowledged (information security risks resulting from legacy hardware, legacy system support and the inherited ICT estate) and measures are in place to close these, the Keeper’s agreement is on an ‘improvement model’ basis on the condition he is updated on progress.</p>
<p>9. Data Protection</p>	<p>A</p>	<p>G</p>	<p>The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law.</p> <p>The <i>Management of Records SOP</i> (page 9) states “Data protection legislation requires PS to retain personal data for no longer than is necessary for the purpose for which it is processed.”</p> <p>Police Scotland have a <i>Data Protection Policy</i> (version 2.0 dated February 2018), which is published on their website. The <i>Data Protection Policy</i> confirms that Police Scotland “recognises the need to ensure that the rights and freedoms of individuals are considered in the processing of personal data.” and “will ensure that all processing of personal data is undertaken in accordance with the Data Protection Act 2018 and the General Data Protection Regulation.”</p> <p>The <i>Data Protection Policy</i> is supported by the <i>Management of Records SOP</i>, <i>Data Protection SOP</i> and <i>Subject Access Request SOP</i>, which provide guidance and instruction to staff. All of which have been provided as evidence. These are available to staff on the intranet and published on the Police Scotland website, Standard Operating Procedures - Police Scotland. The <i>Data Protection SOP</i> (version 8.00 dated June 2021) explains the 6 principles of the Data Protection Act 2018.</p>

			<p>The Keeper notes the <i>Data Protection SOP</i> is currently undergoing approval after being updated in to include SAR information.</p> <p>Privacy notices are published on Police Scotland’s website, Privacy Notices - Police Scotland and include information and guidance for the public on their rights under data protection legislation. They explain how to make a Subject Access Request (SAR) and Individual Rights Requests (IRRs), such as the right to erasure. The governance and reporting of both SARs and IRRs is explained in the <i>RMP</i>. SAR compliance rates are reported to the Audit and Risk Board and IRRs are monitored by the DGB.</p> <p>An Information Charter is also published on the website which outlines the authority’s commitment to data protection legislation, Information Charter - Police Scotland.</p> <p>The IAR acts a record of processing for information assets containing personal data. An <i>extract of the IAR</i> has been provided.</p> <p>The Chief Constable of the Police Service of Scotland, as data controller, is registered with Information Commissioner (Registration number: Z3611656, Expires: 26 March 2023).</p> <p>Police Scotland have a Data Protection Officer and a job description for this post has been provided.</p> <p>All staff receive Information Management input induction training on commencing employment. This training must be completed before staff are given access to the network. As noted at element 8, staff must acknowledge the Acceptable Use Policy, which includes adherence to data protection legislation, each time they log on to the network. Mandatory annual Data Protection Refresher training for all staff is</p>
--	--	--	---

			<p>undertaken through an online learning platform, with compliance monitored. Evidence has been submitted showing the contents of training modules and staff access to them on intranet site.</p> <p>Data Protection Impact Assessments are mandatory for new ICT systems and required for any new processing of personal information. A staff communication from the ACC Professionalism and Assurance (named at element 1) was issued to highlight this process, a copy of which has been provided. A <i>DPIA template</i> has been provided and figures illustrating uptake of the process are noted in the <i>RMP</i>.</p> <p>In relation to processing Individual Right’s Requests, while there is an established process to deal with such requests through the Information Assurance Team and IAOs, Police Scotland note that “at times the decision to uphold an applicant’s request does not result in deletion of the data due to some systems being identified as not capable of destruction because of underlying architecture or reliance of other systems.” (<i>RMP</i> page 22). The Keeper acknowledges the issues around legacy line-of-business systems (see elements 5 and 6).</p> <p>As noted at element 6, Police Scotland have highlighted that “destruction is not systematic and in areas the force is failing to destroy personal information in accordance with data protection legislation, particularly in relation to legacy systems.” (<i>RMP</i> pages 21-22). This is further noted in the <i>DROG ToR</i> (page 2). As outlined above, the DROG was established to manage the over-retention of records. Work is being undertaken to address this issue through the identification, weeding and destruction of records (Force Weeding Project, regular Divisional Highlight Reports to the DROG, IAR), the identification and replacement of systems for which this is an issue (ICT Systems Lists, Core Operational Solutions, Data Drives Programme and IAR). Police Scotland have further planned work, ‘GDPR Structured and Unstructured Data’, which “aims</p>
--	--	--	--

			<p>to bring in technology that will support the automatic classification of structured and unstructured content to aid with retention and weeding decisions.” Since submission, Police Scotland have separately acknowledged the Keeper’s concerns and stated, “assurances are given that Police Scotland is putting in place measures to deal with the high level of risk caused by the over-retention of information and records.” Furthermore they have outlined the following:</p> <p>“The submitted RMP has detailed the investment in new technology being made under the Data Drives Digital Programme and since submission of this RMP in May 2021... In addition, the work of the DP Reform Project and latterly the DROG has created more awareness across Police Scotland on the subject of over-retention than has previously been the case and the data retention risks are monitored at the highest levels of the organisation.</p> <p>... Police Scotland’s information legacy is complicated, which is effecting the speed at which it can be resolved. However, ... robust governance is in place and the organisation has committed increased resources at several points. Therefore, Police Scotland is in a much better place to improve its position over the course of this RMP lifecycle.</p> <p>To that end, Police Scotland would specifically like to invite the Keeper and his team to visit Police Scotland sometime within the next 12 months for a first-hand account of the impact the new posts and technology have had.”</p> <p>The Keeper welcomes these assurances and the invitation to actively engage further. He is confident Police Scotland are taking the necessary measures to ensure compliance under this element is fully achieved.</p> <p>The Keeper can agree this element on an ‘improvement model’ basis.</p>
--	--	--	---

			<p>Currently Police Scotland are unable to manage all their public records involving personal data in compliance with data protection law. However, work is being undertaken and further work is planned to address this. This agreement is conditional on the Keeper being updated on progress.</p>
<p>10. Business Continuity and Vital Records</p>	G	G	<p>The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.</p> <p>Police Scotland are required to have a Business Continuity Management System in place to ensure continued delivery of service due to their status under civil contingency legislation (<i>RMP</i> page 31).</p> <p>Police Scotland's Business Continuity Plans (BCPs) are in place for every function that supports strategic priorities, such as 'Command and Control Communications' and 'Operational Policing'. The <i>RMP</i> (page 31) notes, "Each plan is based on an assessment of the risk to disruption of key processes, and details the contingencies to address the loss of their information and communication systems, as well as loss of accommodation, facilities, people and support chains."</p> <p>A Police Scotland <i>Business Continuity Plan template</i> has been submitted in place of redacted completed plan. Police Scotland have confirmed separately that this "provides the framework for business continuity arrangements required from each local policing/business area." System/record recovery is featured in section 8.3 where there is a requirement to "record technical manuals, emergency plans, maintenance contracts etc." and "the locations of physical documentation/records and locations of Force IT systems." It has further been confirmed separately that, "In addition each plan requires that the locations of 'battle boxes/grab bags' are recorded; these contain vital hard copy records required to facilitate continuity of operations."</p>

			<p>A <i>Business Continuity Management Divisional Guidance</i> (version 1.00 dated January 2021) document provides information and instruction for staff on creating, implementing and maintaining BCPs. This is available on the staff intranet site and a screenshot showing this has been provided.</p> <p>Individual BCPs are reviewed annually for each business area and new elements developed, such as a Severe Weather Plan. Business Continuity Coordinators for each business area are responsible for ensuring BCPs remain fit for purpose. In addition to annual reviews, BCPs are routinely 'exercised' to highlight areas for development. This was last done in March 2020 in preparation for Covid-19, resulting in the development of COVID-19 BCPs. A copy of the <i>BCM 2020-2021 Exercise Programme</i> has been provided. A further exercise is planned for 2022-23 with a focus on potential network and ICT failures as a result of the increase in cyber-security incidents (see comments at element 8) and threat of power outages.</p> <p>Internal audit is also utilised to review the effectiveness of BCPs and their compliance with Police Scotland requirements and BS ISO 22301. (<i>Business Continuity Management Divisional Guidance</i> page 12).</p> <p>The <i>ICT Backup Policy</i> explains the process for the recovery of digital records stored on Police Scotland networks. The <i>RMP</i> (pages 25-26) notes that off-line backups are also being developed.</p> <p>Disaster recovery support is in place for hardcopy records held onsite. This service is supplied by a specialist record salvage and recovery company, Harwell Restoration. A <i>Harwell Priority User Certificate</i> has been supplied as evidence. The Keeper can agree provision is in place for the recovery of hardcopy records.</p> <p>Business continuity processes are in place at third party offsite storage. The following documents have been provided to demonstrate the requirements met by</p>
--	--	--	---

			<p>the successful supplier in relation to business continuity, <i>Invitation To Tender (ITT) for the contract (section 5.20), and part 7 of the Technical Response document.</i></p> <p>Vital records are identified in the IAR. An extract of the <i>IAR Vital Column</i> has been provided. The <i>Record Retention SOP</i> (page 2) also lists the identification of vital records for business continuity as an objective.</p> <p>A staff awareness campaign was planned to run in conjunction with the Business Continuity Institute Awareness Week for 2021. This is commended by the Keeper. Police Scotland have confirmed separately that this campaign took place with emails sent to Divisional business continuity coordinators containing links to awareness videos and the Business Continuity Institute's website.</p> <p>Staff business continuity training was paused due to Covid-19, and plans are in place for this to be delivered online due to staff working remotely.</p> <p>The Keeper acknowledges and commends the listed planned developments, which include the creation of BCC Forums and an ICT Disaster Recovery Plan. The planned work with procurement to include clauses relating to BC in supplier contracts is also noted. The Keeper would like to be updated as this planned work progresses.</p> <p>The Keeper agrees Police Scotland have an approved business continuity management system in place and identifies vital records. He also agrees that information management and records recovery properly feature in the authority's plans.</p>
11. Audit trail	A	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>Management of Records SOP</i> (page 3) states “In order to manage records effectively, it is important to be able to identify them.”</p> <p>Police Scotland explain arrangements for the different formats of records they create and manage:</p> <p><u>Digital - Shared Drives:</u> Police Scotland acknowledge the limitations for audit trail in shared drives (<i>RMP</i> page 33). The introduction of UAM (noted at element 4) ensures greater access control to folders in shared drives. The Records Management Team can now provide reports to business areas on their users. As explained below naming convention and version control procedures are in place.</p> <p><u>Digital – ERDMS/SharePoint:</u> SharePoint is noted as being in use (<i>RMP</i> page 33). It has a powerful search function and version control. The Keeper notes that an ERDM system is being introduced in one business area and will be rolled out more widely. This will of course bring greater audit control capabilities as it will likely have built in version control and an effective search facility (see element 4).</p> <p><u>Digital – Line-of-business systems:</u> Audit and tracking functionality is not available in all line-of-business systems in use. The <i>RMP</i> (page 34) explains that in response to new data protection legislation in 2018 work was undertaken to identify and decommission or update systems which did not have the required retention, weeding and tracking functionality. This work identified critical systems and is being developed through the ICT Systems List to include all systems containing public records. Those systems originally identified are being updated through the ongoing Core Operating Solutions (COS) programme. This work is overseen by the DROG. Audit trail is considered with the introduction of new</p>
--	--	--	---

			<p>ICT systems.</p> <p><u>Hard-copy onsite:</u> Records stored onsite across the Police Scotland estate are indexed and indexes saved to the appropriate shared drive area or ICT-supported system. A register is maintained to manage movement of and access to these records (<i>Management of Records SOP</i> page 5). A Divisional Highlight Report template, which each senior management representative is required to submit to bi-monthly DROG meetings, includes tasks (Part 2 Section A) to ensure the location of onsite hardcopy records is tracked and recorded. A <i>sample DROG Highlight Report</i> has been provided.</p> <p><u>Hard-copy offsite:</u> The offsite storage of hard-copy records by third party providers has been rationalised by using one single provider. This involved the migration of 12,000 boxes and work is ongoing to transfer a further 7,000 boxes. As noted under elements 4 and 5, an online portal allows identified and trained individuals in each business area to oversee records stored, access inventory reports and tracks the movement of records. A sample <i>Offsite Storage Supplier Box Transaction History</i> has been provided. When records are transferred back to Police Scotland premises they are subject to the same tracking and access process (use of a register) as noted above for hard-copy onsite records. The Highlight Report template mentioned above, includes tasks (Part 2 Section B) to ensure the location of offsite hardcopy records is tracked and recorded. Staff guidance on offsite storage box marking and indexing is included in the <i>Management of Records Divisional Guidance</i> (section 4). The <i>Home Working – Information Security</i> document, noted at element 8, includes guidance on maintaining an audit trail of records taken offsite when staff are working remotely.</p> <p>Police Scotland have file and folder naming conventions and version control processes and staff guidance. These are outlined in the <i>Management of Records</i></p>
--	--	--	---

			<p><i>Divisional Guidance</i> (section 3) and apply to all records regardless of format or location. The Keeper agrees that this gives clear and appropriate instructions to staff to ensure that records are named in a way that allows tracking and version control. A screenshot showing a link the <i>Management of Records Divisional Guidance</i> on the staff intranet site has been provided.</p> <p>Lawful Business Monitoring (LBM) is also in use as an audit tool. It is utilised in certain controlled circumstances and “monitors and records all computer based actions carried out by users on the network...” (<i>RMP</i> page 34)</p> <p>As noted at element 3, the Keeper acknowledges the highlighted risks resulting from the differing processes for creation, approval, management and review of SOPs and guidance documents. The <i>RMP</i> (page 9) states “The issue of Divisional Guidance presents a risk to the effective management and governance of the Police Scotland record set and to the assurance that accurate version control and version history are in place.” The Keeper notes that work is planned to mitigate these risks.</p> <p>As noted above, planned developments for line-of-business systems/unstructured data are underway in the form of the COS programme and ICT Systems Lists. This work “will aid in the planning and prioritising of the decommissioning or remediation of systems that lack the appropriate level of audit detail whether that be due to PRSA, GDPR or DPA requirements.” (<i>RMP</i> page 35). The planned Data Drives Programme will include a ‘Metadata Management’ project that will look at the use of “technology to increase audit capabilities” (<i>RMP</i> page 12). Further planned work includes updating the <i>DROG TOR</i> to feature wider audit trail considerations. Police Scotland have committed to updating the Keeper on progress of this work.</p>
--	--	--	---

			<p>The Keeper can agree this element on an 'improvement model' basis as Police Scotland have identified a gap in provision (a lack of audit trail functionality in line-of-business systems/structured data; the process for development of divisional guidance documents) and work has been identified and is underway to address this. This agreement is conditional on the Keeper being updated on progress, which Police Scotland have committed to doing.</p>
<p>12. Competency Framework for records management staff</p>	<p>G</p>	<p>G</p>	<p>The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.</p> <p>Police Scotland have mandatory training in place for all staff and additional training in place for staff with information management roles, "All Officers and Staff must attend Information Management training input prior to being given access to ICT systems and regularly undertake PS's mandatory Data Protection training to ensure that they are aware of responsibilities in this area. Specific training will be provided by Records Management prior to individuals being given access to records management systems of external storage suppliers." (<i>Management of Records SOP</i> section 13).</p> <p>All staff are required to complete Information Management Input training when they commence employment and before they are given network access (see element 9). A copy of the slide deck for this training and an overview of the content have been provided. All staff must complete annual Data Protection Refresher training (see element 9). A screenshot showing access to this training on the staff Moodle and a synopsis of the content have been supplied. All staff receive an information security induction when they are employed (see element 8).</p> <p>Business Continuity training was paused due to Covid-19 and plans are in place to recommence using online training while staff work remotely (see element 10).</p>

			<p>The SIRO (named at element 1) and Strategic Information Asset Owners (IAOs), who support this role, receive role specific training from the Records Manager and Information Security Manager (see element 1). This training is “delivered in person, 1-2-1 with each SIAO by the Records Manager, Information Security Manager and the Information Manager (Assurance)”. (<i>RMP</i> page 39)</p> <p>One-off training was provided to Information Assurance Officers (IAOs), who did not have a professional qualification in records management, in 2019 by an external trainer. A copy of the training slides has been provided.</p> <p>Role specific training is provided where necessary, for example in relation to information sharing (see element 14).</p> <p>The <i>RMP</i> notes the development and delivery of further training and guidance for SIAOs and IAOs under the development plan section. The Keeper would welcome updates in PUR submissions on the development and delivery of any new training.</p> <p>The Records Manager role is supported by staff with specific information management responsibilities. Several of these staff members are professionally qualified in archives and records management.</p> <p>The Keeper would be interested in an update on the qualifications of the new Records Manager when appropriate.</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, he agrees that Police Scotland consider information governance training for staff as required.</p>
13.	G	G	Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review.

<p>Assessment and Review</p>			<p>Police Scotland commit to carrying out a formal annual review and assessment of their <i>RMP</i> which will be aligned with the annual, voluntary, NRS Progress Update Review process. The <i>Letter from the Accountable Executive Officer</i> supports this commitment.</p> <p>Compliance with PRSA will be regularly reported to the Data Governance Board (DGB) (see General Comments), including Progress Update Reviews and progress under this element of the <i>RMP</i>. The DGB is chaired by the ACC Professionalism and Assurance (named at element 1) and attended by the Records Manager (see element 2). It is “the forum where data/information governance matters are reported.”(<i>RMP</i> page 38). The <i>DGB Terms of Reference</i> have been provided.</p> <p>There is also an annual review commitment under most elements of the <i>RMP</i>. For example, “Progress on this element will be included in the annual revision of the Plan, which will be provided to the Keeper of the Records of Scotland as part of the Progress Update Review mechanism.” (<i>RMP</i> page 35)</p> <p>The Records Manager post has overall responsibility for carrying out assessment and review. This is noted in several documents submitted to the Keeper, for example, the Records Manager <i>Job Description</i> indicates this responsibility under section 3 points 3, 7 and 8; and the <i>Records Retention SOP</i> (section 3) notes that the Records Manager is responsible for its regular review. Where required, the Records Manager will draw on the additional roles in Information Assurance and other departments “in order to provide independent assessment to support those reviews.” The <i>RMP</i> (page 7) notes the responsibilities of the Records Officer post, which supports the Records Manager post, include developing and reviewing the <i>RMP</i>.</p> <p>The <i>RMP</i> explains the methodology used to carry out review and assessment. The</p>
------------------------------	--	--	--

		<p>resulting information is used by the Records Manager to assess implementation of the <i>RMP</i>. Three main methods currently in use by the Records Manager:</p> <ul style="list-style-type: none"> • Reports - reporting tools are accessed by the Records Management Team to provide information on mailbox sizes, SharePoint Sites, Network Folders, Off-Site Storage, etc. Regular reporting to the DROG through the use of divisional highlight reports (see elements 4, 5, 6, 9 & 11 and General Comments), which monitor and assess work around the availability of records, identification of records to be added to the IAR and progress on compliance around retention and disposal of records in each division. The report template is structured around set questions and contains sections covering all formats of records along with instructions for completion. The <i>RMP</i> states, "Access to this level of information helps ensure a robust review across a number of elements of the RMP such as Elements 4, 5 and 6." • Direct Oversight – Ongoing review and assessment of implementation of elements 6 and 7 are directly overseen by the Records Management team. This is done through the use of destruction authorisation forms (see elements 5 and 6) and the Records Manager's direct oversight of relationships with partner archives (<i>RM Job Description</i> point 3.1). The <i>RMP</i> states, "Direct oversight would also hold true for Elements 1, 2, 3, 4, 5 and 12." • Business Area Leads – The <i>RMP</i> notes "The remaining elements (8, 9, 10, 11, 14 and 15) are covered through the involvement of Business Area Leads who lead on all or some aspect of each element." <p>The <i>Management of Records SOP</i> (section 2) notes that Information Assurance, of which the Records Management Team are part of, are "Responsible for assessing compliance through regular information audits." Police Scotland have confirmed separately that "the Information Security Manager maintains a schedule of audits that Information Assurance undertakes for Police Scotland, which is based and prioritised on the level of information risk. That schedule does include audits</p>
--	--	--

			<p>assessing compliance with the Force's information management related Standard Operating Procedures, but it must be noted that conducting regular audits across the full schedule is limited by available resources. Further audits are based on the number of errors found/highlighted or non-compliances discovered through various means such as Information Security Incidents.”</p> <p>The use of internal audit to assess compliance is also evident and has been utilised to identify areas for review and improvement. In particular, around retention in an internal audit report produced in June 2020 (<i>RMP</i> pages 15 and 23). The use of internal audit is commended by the Keeper. Furthermore, audits and monthly reporting are in place to assess information sharing (element 14). The <i>RMP</i> states regular audit and inspection is carried out across Police Scotland business areas and, where records and information are concerned, the Records Manger is involved and will use these to inform assessment.</p> <p>Police Scotland are working towards compliance with the Scottish Government Cyber Resilience Framework, which includes a self-assessment tool (see element 8).</p> <p>While supporting documents have a version control table, this does not always include a review period or date. A copy of the <i>Governance of the Police Scotland Record Set Guidance</i> has been supplied. This notes (page 8) that reviews will either be cyclical or casual. As noted at element 3, the Keeper acknowledges highlighted risks resulting from the differing processes for creation, approval, management and review of SOPs and guidance documents. The Keeper notes work is planned to mitigate these risks.</p> <p>The Keeper acknowledges that a strategic review of all SOPs took place in 2019 and other reviews are highlighted, for example a comprehensive review of the Information Security Policy (<i>RMP</i> page 25). BCPs are reviewed annually and</p>
--	--	--	---

			<p>subject to regular test exercises (<i>RMP</i> page 31).</p> <p>The Keeper agrees that Police Scotland have made a firm commitment to review their <i>RMP</i> as required by the Act and have explained who will carry out this review and by what methodology. Furthermore he agrees that supporting policy and guidance documents are appropriately reviewed.</p>
14. Shared Information	G	G	<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>Police Scotland state information sharing is carried out “where it is relevant, necessary and proportionate to do so and in line with its statutory and regulatory obligations.” (<i>RMP</i> page 39)</p> <p>This is achieved through the use of DPIAs, for example when information is shared internally between different systems. Access controls are in place to ensure access to network folders and mailboxes is based on individual roles and is monitored (see elements 4 and 8).</p> <p>Police Scotland share information with a range of third party organisations, “Routine and regular sharing of information with other bodies is essential to effective operational policing and procedures are in place to govern regular information sharing.” (<i>RMP</i> page 40)</p> <p>Information Sharing Agreements (ISAs) are in place to manage these arrangements and any new information sharing is subject to a DPIA. A reviewed and approved ISA corporate process “to request, track and approve such an agreement” is now in place after a review in 2018. A sample <i>Information Sharing Agreement Template</i> has been provided.</p>

			<p>Police Scotland are currently looking at creating framework agreements with Local Authorities and the NHS to streamline this process. A copy of a template <i>Letter from the ACC to Local Authority CEOs</i> had been provided. It has been confirmed separately that this work has progressed since submission. A draft document was circulated in June 2022 for consultation by all partners, with Glasgow City Council, as lead partner on behalf of the 32 local authorities. The Keeper requests he is updated as this work progresses further.</p> <p>An <i>Information Sharing SOP</i> (version 3.00 dated September 2019) provides guidance and instruction for staff, and includes a series of process flowcharts. A copy has been provided. Staff can access this on the guidance section of the staff intranet. A screenshot showing this has been provided.</p> <p>Information sharing for academic and research purposes is managed through a process developed between the Academic Research Team and Information Governance. A copy of slides outlining the workflow for this process has been provided.</p> <p>Police Scotland have an Information Sharing Register, which is managed by Information Assurance. A copy of <i>ISA-Register IM-Dashboard-View</i> has been provided. The <i>Information Sharing SOP</i> (point 10.5.4) notes all ISAs will be reviewed annually.</p> <p>One-off information sharing is also necessary in operational policing and the process for managing this using a single national form is explained. Guidance on this is included in the <i>Information Sharing SOP</i> (section 8) and support is available from the Information Assurance Team if required. A copy of <i>Form 052-003 Request for Disclosure of Personal Data from External Organisations</i> has been provided.</p>
--	--	--	---

			<p>Police Scotland has provided an explanation of governance arrangements for information sharing. Each SIAO is responsible for ensuring appropriate arrangements are in place and the ACC Professionalism and Assurance (see element 1) oversees information sharing.</p> <p>Police Scotland recognise information sharing as an organisational risk and it is the subject of monthly reporting to senior staff and the DGB. A sample <i>Information Sharing Risk Register Entry</i> has been provided. Work to mitigate risk has been carried out, including a maturity assessment review. The Keeper notes the ongoing and planned work around information sharing risk.</p> <p>Information sharing is part of the training is provided to SIAOs (see elements 1 and 12) and specific training is provided where required, for example to officers involved in sharing information relating to individuals experiencing vulnerability.</p> <p>The Keeper can agree that Police Scotland 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 Act expects a public authority to ensure that adequate arrangements are in place for the management of records created and held by third parties who carry out any functions of the authority.</p> <p>The <i>RMP</i> (page 42) states “Police Scotland functions are not carried out by a third party, however as mandated in the Management of Records SOP, any such instances where this does occur must be referred to Records Management to ensure that records created or held by a third party carrying out a Police Scotland function are managed to the satisfaction of Police Scotland, to ensure that statutory obligations are met.”</p> <p>As noted above, the <i>Management of Records SOP</i> (section 14) confirms this, “PS</p>

			<p>functions are generally not carried out by a third party (e.g. contractor), however any such instances where this does occur must be referred to Records Management to ensure that records created or held by the third party carrying out the function are managed to the satisfaction PS. PS's statutory obligations under the Freedom of Information and Data Protection Legislation extend to such records."</p> <p>While Police Scotland are clear none of their functions are carried out by a third party, provision is included in templates for invitation to tender and contracts to ensure compliance with freedom of information and data protection legislation. A <i>Contract Terms Template</i> has been provided, which includes records management provisions (section 18), and specifically mentions "obligations under the Public Records (Scotland) Act 2011 and with the Authority's Records Management Plan..."</p> <p>The <i>RMP</i> (page 42) highlights the relationship between Police Scotland and its governing body, the Scottish Police Authority (SPA), which is managed by the Police and Fire Reform (Scotland) Act 2012. In particular the provision of forensic services by SPA for Police Scotland. This is not considered by the Police Scotland Records Manager as "constituting public records being created by a third party."</p> <p>The Keeper accepts that this element is not applicable to Police Scotland and acknowledges the commitment to inform him of any relevant changes.</p>
--	--	--	---

General note on submission:

Version:

This assessment is on the Police Scotland Records Management Plan (the *RMP*) submitted to the Keeper for his agreement on 28 May 2021. This is version 2.0 of the *RMP* dated 28 May 2021. The *RMP* is approved by the Assistant Chief Constable Professionalism and Assurance (see element 1). The Keeper originally agreed the *Records Management Plan* of Police Scotland in 2014: [Police Scotland Assessment Report \(nrscotland.gov.uk\)](#); the authority submitted a Progress Update Review (PUR) in 2019: [Police Scotland \(nrscotland.gov.uk\)](#).

The authority refers to records as a vital asset (for example *Management of Records SOP* page 2). This is an important recognition and the Keeper commends it.

“Records Management issues must be taken into consideration when planning or implementing ICT systems, when extending staff access to new technologies and during restructuring or major organisational changes, to ensure that record keeping requirements are met from the start of such new processes.” (*Management of Records SOP* page 4). The Keeper commends the alignment of records management with the development of new technologies and organisational change.

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>

Key Group: Data Governance Board (DGB)

The Board was established in May 2020 replacing the Information Governance Board. It meets quarterly and is chaired by the Assistant Chief Constable Professionalism and Assurance (see element 1). The Records Manager is a member of the DGB. The *Data Governance Board Terms of Reference* state the purpose of the DGB is “to provide Data Protection Governance for Police Scotland and be the decision making body for information assurance matters, including Records Management, Information Security, Information Sharing and Data Standards. The Board will have responsibility for agreeing policy and procedures to ensure compliance with legislative and regulatory obligations”. Its remit includes “Strategic oversight of the application of legislation (e.g. Data Protection, GDPR, Public Records (Scotland) Act)”. In addition, “It remains the forum where data/information governance matters are reported and specifically where PURs will be submitted annually.” (*RMP* page 37). Strategic Information Asset Owners (SIAOs) can report matters to the DGB.

Local Records Management:

The three levels of Information Asset Ownership are explained along with their roles and responsibilities in the *Information Assurance SOP*:

- Strategic Information Asset Owner (SIAO) (Member of Force Executive)
- Tactical Information Asset Owner (TIAO) (Chief Supt / Supt / Staff in appropriate post / grade)
- Operational Information Asset Owner (OIAO) (All officers / staff)

SIAOs support the Accountable Executive Officer (element 1) and are provided with training carried out by the Records Manager (element 2), Information Security Manager and Information Manager (Assurance). A *Letter from the Accountable Executive Officer* specifically address SIAO training and their role and how the feedback to Information Assurance.

The *Management of Records SOP* (section 2) outlines roles:

Information Assurance – “Responsible for assessing compliance through regular information audits.”

Information Asset Owners – “Responsible for ensuring that records created by their areas are managed in line with this SOP”

The *Retention of Records SOP* (section 3) notes Strategic and Tactical Information Asset Owners are “Responsible for ensuring that records falling within their remit are managed in line with this SOP.”

The *Information Security SOP* (section 3) notes SIAOs “are the business owners of the information within their areas of responsibility and are responsible for the effective use and protection of the information they are responsible for.”

The *Data Protection SOP* (section 15) notes the role of SIAOs with regard to the record of processing activities, “All Strategic Information Asset Owners have access to the IAR and are responsible for ensuring the entries therein are up-to-date, supported by the Records Manager”.

Data Retention Oversight Group (DROG) – This group was developed out of the Data Retention and Review Design Authority which had been established in advance new data protection legislation in 2018. It is chaired by ACC (element 1) and attended by the Records Manger (element 2) and is “driving forward improvement in retention and weeding.” The DROG reports to the DGB and its *Terms of Reference* states it “will provide Police Scotland with a multi-disciplinary forum to prioritise and manage the work required by every business area to meet legislative and regulatory requirements in respect of structured, unstructured and hard copy data. It will coordinate data retention across the Force, be a platform to share good practice and inform the deployment of the Weeding and Retention Group.” There are bi-monthly meetings at which senior management representative from each business area are required to submit divisional highlight reports. These reports provide updates on progress of ongoing work. In addition, local data retention sub-groups have been established in departments/divisions to progress work outlined by the DROG.

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

Elements that require development by Police Scotland are as follows:

4. Business Classification
5. Retention schedule
6. Destruction Arrangements
7. Archiving and Transfer
8. Information Security
9. Data Protection
11. Audit trail

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper **agrees** the RMP of **Police Scotland**.

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

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



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



.....
Paul Lowe

Keeper of the Records of Scotland