National
Records of
Scotland

Public Records (Scotland) Act 2011

Police Scotland
Assessment Report

The Keeper of the Records of Scotland

16 Dec 2014

Contents

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came fully into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor record keeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Executive Summary

This report sets out the findings of the Keeper's assessment of the RMP of Police Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 30 September 2014***.***

The assessment considered whether the RMP of Police Scotland was developed with proper regard to the 14 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 formally established on 1 April 2013 and is responsible for policing across the length and breadth of Scotland, some 28,168 square miles. The Service is led by Chief Constable Stephen House and comprises police officers, police staff and special constables who are working together to deliver the best possible policing service for the people of Scotland. The Chief Constable is supported by a command team of 4 Deputy Chief Constables, Assistant Chief Constables and 3 Directors.

Police Scotland’s purpose is to improve the safety and wellbeing of people, places and communities in Scotland.

There are 14 local policing divisions, each headed by a Local Police Commander who ensures that local policing in each area is responsive, accountable and tailored to meet local needs. Each division will encompass response officers, community officers, local crime investigation, road policing, public protection and local intelligence.

The corporate interim headquarters of Police Scotland is based at Tulliallan in Fife which is also where the Scottish Police College is based, the training home of Police Scotland.

Police Scotland took over responsibility for policing in Scotland from the eight former police forces, the Scottish Crime and Drug Enforcement Agency and the Association of Chief Police Officers in 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 *Compulsory element*	G	G	The senior officer responsible for records management within Police Scotland (PS) has been named as Deputy Chief Constable (Designate) Neil Richardson. Mr Richardson is the Senior Information Risk Owner (SIRO) for PS. He is supported in this by the four Assistant Chief Constables and four Executive Directors who are Information Asset Owners for their relevant areas. Mr Richardson Chairs the Corporate Governance Board. The Information Asset Owners also sit on the Board, which was established in May 2014 and sits quarterly. Its purpose is to consider the levels of information risk facing PS as well as assessing records management provisions. This is evidenced by a letter from Mr Richardson accompanying the submission of PS's Records Management Plan (RMP) (Evidence 1.1). The Keeper agrees that Mr Richardson is an appropriate individual to take senior responsibility for records management.
2. Records Manager *Compulsory element*	G	G	Head of Information Management, Iain Gray, has been identified in the letter (Evidence 1.1) from Mr Richardson (see Element 1) as the individual responsible for the day-to-day operation of records management within PS. Mr Gray reports information management issues to the Corporate Governance Board. The Role Profile and Job Description of Mr Gray have been submitted as evidence (Evidence 2.1). It states that Mr Gray is responsible for developing, implementing

	🟩	🟩	and monitoring an Information Management Strategy and information management policies to meet the business requirements and legal obligations on Police Scotland. The Role Profile and Job Description also set out where Mr Gray appears on the Organisational Chart of the Information Management area of business within PS. The Keeper agrees that Mr Gray is an appropriate individual to take operational responsibility of records management.
3. Policy *Compulsory element*	**G**	**G**	PS have submitted their Records Management Policy (Evidence 3.1). The Policy sets out PS's strategic approach to records management, showing their commitment to managing the records they create and receive as well as outlining the roles and responsibilities of staff for adhering to the policy. Evidence 3.2 shows that the policy has been approved by the SIRO (see Element 1). The Policy is intended to be a high level document supported by a suite of standard operating procedures. These are: Record Retention standard operating procedure (Evidence 3.3) – this document sets out the procedures for determining the retention periods applied to types of records created by PS. This is a very detailed practical document. It also highlights the requirement under the s.61 Code of Practice of the Freedom of Information (Scotland) Act 2002 to keep a record of records that are destroyed. The document also recognises the differing practices that were in place in the territorial forces prior to reorganisation in 2013 and the difficulties in standardising practice across the new organisation. Secure Destruction and Disposal of Data standard operating procedure (Evidence 3.4) – sets out the practical procedures for ensuring that paper records, hardware and electronic storage devices are securely disposed of to appropriate standards.

	🟩	🟩	ICT Systems Development standard operating procedure (Evidence 3.5) – highlights the need to incorporate information management requirements into planning for new ICT systems/projects. Management of Records standard operating procedure (Evidence 3.6) – provides staff guidance on records management principles such as file naming conventions, version control, management of drives and email management. Storage of Records standard operating procedure (Evidence 3.7) – sets out guidelines for storage of paper records. Also submitted as evidence is the Information Management Policy Framework (Evidence 3.8) which is a useful document bringing together the different strands of information management within PS. The Policy and associated standard operating procedures, policies and guidance are available to all staff on the guidance section of the PS intranet. Several of the standard operating procedure documents have appendices which detail the different practices used by the predecessor organisations of PS. The Keeper notes this approach is appropriate as PS moves towards standardisation of its procedures. The Keeper agrees that a corporate approach towards records management is outlined in the Records Management Policy and this is supported by appropriate procedural documents.
4. Business Classification	**A**	**A**	PS has submitted evidence of classification schemes from predecessor bodies (ACPOS and Strathclyde Police, Evidence 4.1 and 4.2 respectively). This shows that some kind of classification was in place until PS came into being in 2013. These are still in operation until a standardised approach can be developed.

	🟧	🟧	Work is ongoing in streamlining the functions of PS and the Scottish Police Authority and until that work is finalised PS is unable to fully identify the functions it will be required to undertake. Proposals have been made, and accepted by the Senior Leadership Board (Evidence 4.3 and 4.4), to appoint 6 Assistant Chief Constables and 4 Executive Directors as Information Asset Owners (IAOs). PS proposes that its classification scheme is based on the portfolio areas of the IAOs as this functional structure should be more stable than a divisional one. PS has stated that none of PS's functions are carried out by a third party. Support services provided to PS are done so on a contractual basis and, as part of a review of these contracts, they will include relevant provisions for data processing and records management. The Keeper commends this approach. The RMP states that progress towards developing the classification scheme will be reviewed annually and that the Keeper will be kept informed of this. The Keeper commends this approach. The Keeper can agree this element on an 'improvement model' basis provided he is kept informed of progress towards developing a business classification scheme.
5. Retention schedule	G	G	As evidence, PS has submitted their Record Retention standard operating procedure (Evidence 3.3). This document sets out the procedures for determining the retention periods applied to types of records created by PS. This is a very detailed practical document. It also highlights the requirement under the s.61 Code of Practice of the Freedom of Information (Scotland) Act 2002 to keep a record of records that are destroyed. The document also recognises the differing practices that were in place in the territorial forces prior to reorganisation in 2013 and the difficulties in standardising practice across the new organisation. The geographical

			appendices set out the variations in practice. Also submitted is an example of the regular destruction (Evidence 5.1) that takes place using the retention schedule as a basis. The Record Retention standard operating procedure is available to staff on PS's intranet system. The retention schedule within the document will be kept under review to ensure it meets the needs of PS. The RMP states that the procedures for recording the disposal of records will be standardised and distributed to staff as a standard operating procedure. The RMP also states that the schedule will be reviewed annually to ensure that it is fit for purpose and any changes will be intimated to the Keeper. The Keeper agrees that PS has an operational retention schedule in place and welcomes the commitment to continually review this as the organisation continues to standardise its policies, practices and procedures.
6. Destruction Arrangements *Compulsory element*	**G**	**G**	The current arrangements for the secure destruction of PS records are presently under review. PS has inherited a range of different contractual arrangements for the confidential destruction of information from legacy forces and these comprise the current arrangements until the review has been completed. **Paper** PS has submitted a sample of evidence showing that arrangements are in place to securely destroy paper records at the end of their lifecycle. Submitted as evidence are the agreement between the former territorial police force of Tayside Police (now Tayside Division) and a commercial paper shredding firm (Evidence 6.3) and destruction certificates confirming the destruction of paper records at stations in the Tayside area (Evidence 6.4).

	🟩	🟩	**Electronic** PS has submitted evidence (Evidence 6.4) that the deletion of electronic records is undertaken in a systematic and secure fashion. **Hardware** PS has submitted the Secure Disposal and Destruction of Data standard operating procedure (Evidence 3.4) as evidence. This document sets out what appears to be very robust procedures for securely disposing of electronic storage media, which is carried out by an external contractor. Where storage media can be re-used internally, secure 'sanitisation' is carried out by PS ICT department. This is done using the HM Government Infosec Assurance Standard 5, Secure Sanitisation. Destruction or sanitisation processes are documented so that an audit trail is maintained. A sample hardware destruction certificate has been supplied (Evidence 6.5). **Back-ups** The back-up overwriting process is described in System Back-Up and Recovery standard operating procedure (Evidence 10.3). This shows that the back-ups are routinely overwritten, ensuring that records stored on these are disposed of. The Keeper agrees that appropriate procedures are in place to ensure the secure destruction of records.
7. Archiving and Transfer *Compulsory element*	**G**	**A**	PS has submitted a Schedule of Archival Arrangements Sep 14 document (Evidence 7.1) as evidence of the arrangements that are currently in place for archival records created by predecessor forces and bodies. Some forces have agreements in place and others need to have agreements drawn up with the relevant local authority archive service. The RMP commits PS to updating the documentation which governs the transfer arrangement to provide a more standardised approach and to create documentation where none currently exists.

	🟩	🟧	The Keeper commends this commitment. PS will also undertake an audit of historical records currently in their custody to determine their suitability for transfer to the relevant archive. Also submitted as evidence is a Transfer Schedule which shows the transfer of records from Grampian Police and other predecessor organisations to Aberdeen City Archives (Evidence 7.2). PS has agreed in principle to deposit archival records of the unified service dating from 1 April 2013 and later to the National Records of Scotland (NRS). The RMP states that a formal transfer agreement will be developed to set out transfer arrangements. PS will also create an archiving procedure in line with the Information Management policy framework. This will aid the standardisation of procedures for the transfer of archives to either local authority archives or NRS. PS will also identify and implement a solution for the internal archiving of records that are unable to be transferred to external archives due to the sensitive nature of these records. The Keeper recommends that PS adheres to best practice archival standards when developing such a solution. The Keeper can agree that the arrangements for the permanent preservation of records selected for archiving has been considered by PS. He recognises that PS has inherited the responsibility for predecessor bodies’ arrangements and is convinced of PS’s commitment to improve and standardise these procedures, but requests that a formal MoU is progressed for the transfer of archival records from the new body to NRS. He therefore requests that he is kept informed of progress.

8. Information Security *Compulsory element*	**G**	**G**	PS has submitted its Information Security Policy (Evidence 8.1). This document has been approved by the individual named in **Element 1**. The Policy shows PS's strategic approach to information security and is backed up by a suite of standard operating procedures. Information Security standard operating procedure (Evidence 8.3) – sets out staff responsibility for information security and procedures for ensuring information is protected. There is also a commitment to training, with new inductees undergoing training in information security issues and regular training thereafter. The Keeper commends the commitment to regular training as this will ensure that staff have the necessary skills to comply with the policies and procedures. Email and Internet Security standard operating procedure (Evidence 8.4) – this sets out the guidelines for PS staff using email and internet system. It also highlights the importance of not using the email system as a storage area for corporate records. ICT User Access and Security standard operating procedure (Evidence 8.5) – details the arrangements for ensuring security of access to PS systems. Includes the procedures for disabling access to systems when staff leave or retire. Mobile Data and Remote Working standard operating procedure (Evidence 8.6) - this document sets out the procedures to be followed when using mobile devices, storage or working outside the office. Security Incident Reporting and Management standard operating procedure (Evidence 8.7) – this document describes the procedures to be undertaken in the event of a breach of security. The policy and associated procedures are available to all staff through the PS intranet system. These will be reviewed as part of a larger review once the new

			information management staff structure. Any changes to these will be intimated to the Keeper as part of the annual review of the RMP. A report on information assurance, which will included information security assessments, will be submitted to the Corporate Governance Board. PS has submitted a robust policy document which outlines the strategic approach to information security. This is thoroughly supported by a suite of standard operating procedures which clearly set out the steps to be followed in ensuring the security of information created and held by PS.
9. Data Protection	**G**	**G**	PS has submitted their Data Protection Policy (Evidence 9.1). This provides PS's strategic approach to Data Protection and is backed up by practical procedural documents. Subject Access Requests standard operating procedure (Evidence 9.3) – establishes the procedures for dealing with subject access requests. Information Sharing Protocols standard operating procedure (Evidence 9.4) – sets out the procedures to be followed when creating an information sharing protocol. Also supplied is evidence of PS's registration with the Information Commissioner's Office (Evidence 9.5). Induction training is also provided to new members of staff. The notes of the induction training have been supplied as evidence (Evidence 9.6). The Keeper commends this commitment to providing practical training on Data Protection issues. Prior to being able to access any PS information system, staff have to acknowledge a statement of their Data Protection responsibilities.

			PS has also submitted links to an Information Charter section of their website and to a Data Protection area. This clearly indicates to PS's stakeholders how they approach Data Protection. The Keeper commends this approach. PS intends to review these policies and procedures in line with a wider review of information management policies and procedures. Any changes to these will be intimated to the Keeper. Issues of data quality and the management of personal information will be built into the information assurance report to the Corporate Governance Board. The Keeper agrees that PS is aware of its responsibilities under the Data Protection Act and has very robust procedures in place in order to protect personal information.
10. Business Continuity and Vital Records	**G**	**A**	PS requires each Division to create and maintain its own Business Continuity Plan. PS has submitted its Business Continuity Management standard operating procedure (Evidence 10.1). This provides an organisation wide procedure to follow. Testing of business continuity plans is scheduled to take place by March 2015. Progress is monitored by the Corporate Governance Board and a report to this effect has been submitted (Evidence 10.2). PS has also submitted their back-up procedures (Evidence 10.3) and contractual arrangements with a commercial document restoration company (Evidence 10.4). The RMP states that vital records will be identified in partnership with Information Asset Owners and incorporated into business continuity plans. PS has committed to updating the Keeper on progress towards this. The Keeper agrees that PS has processes in place to ensure that it has procedures in place to enable it to resume its key functions in the event of an interruption to its normal business. The Keeper accepts that there is a commitment to identifying vital records and looks forward to being updated as this work progresses.

11. Audit trail	G	A	PS has set out its arrangements for maintaining audit trails for electronic and paper records. **Electronic records** – PS creates most of its electronic records on dedicated databases. The audit trail functionality in these varies due to the differing practices employed by the legacy forces. The ICT Systems Development standard operating procedure (Evidence 3.5, section 5) highlights the need to incorporate information management requirements into planning for new records management systems. Section 3 states that an Information Asset Register will be maintained by the records manager, ensuring that an accurate record of systems in use is maintained. The management of unstructured electronic records is set out in the Management of Records standard operating procedure (Evidence 3.6). It provides guidance on records management principles such as file naming conventions, version control, management of drives and email management. PS's Corporate Strategy 2014 (Evidence 11.1) states that it intends to 'implement controlled electronic records and documents management, subject to a suitable business case and available funding, to improve access to information without compromising the effectiveness of our information security and records management procedures.' This indicates that PS intends to look at the possibility of implementing a standardised system for storing and sharing electronic information. This will form part of a wider 'gap analysis' in information management provision. If the business case is rejected, the Keeper will need to know what PS's plans are for audit trail provision for electronic records. **Paper records -** Management of Records standard operating procedure (Evidence 3.6) and Storage of Records standard operating procedure (Evidence 3.7) – provide staff guidance on records management principles such as file naming conventions, version control, management of drives and email management and for the storage of paper records. PS stores some of their semi-current records off-site with a commercial provider and evidence of the audit trail facilities in place have been

	🟩	🟧	supplied (Evidence 11.2). Hard-copy records storage is also being reviewed and audit trail provision will be considered as part of this. This review is due for completion by April 2015. The Keeper requests he is kept informed of the results of this review. The Keeper agrees that there is some audit trail functionality in place in PS's records management systems. The Keeper welcomes PS's commitment to standardise this across the organisation. He can therefore agree this element on an 'improvement model' basis provided he is kept informed of further developments.
12. Competency Framework for records management staff	G	G	Job descriptions for the relevant staff in the Information management department have been supplied (Evidence 2.1, and 12.1-12.4). These set out the corporate objectives of key staff with regards to information and records management. These include an organisation chart of the Information Management department showing where each member of staff fits in. PS is currently undertaking a consultation with regards to organisational change. The RMP commits PS to informing the Keeper if there are any changes to these job descriptions. Training in records management is recorded in staff's Personal Plan. PS is looking to standardise the methods of recording this. The Keeper agrees that the importance of records and information management is reflected in the job descriptions of relevant staff.
13. Assessment and Review	G	G	PS has committed to annually reviewing the RMP and there are clear statements of intent throughout the RMP to support this. The Corporate Governance Board will assess progress towards meeting the development requirements highlighted in the RMP on a quarterly basis,

			commencing with the next Board meeting in January 2015. PS will consider a self-assessment survey to determine the records management maturity of the organisation. This will then be used to annually assess the RMP. The reviewed RMP will be submitted along with reports to the Corporate Governance Board, to the Keeper. The Keeper agrees that there is a strong commitment to assess and review the RMP to ensure that it continues to meet the needs of PS.
14. Shared Information	**G**	**G**	PS routinely shares information with a variety of public authorities. It has numerous information sharing arrangements in place as a legacy from the predecessor forces. Information Sharing Protocols (ISPs) are drawn up using a standard operating procedure (Evidence 9.4) and is assessed for compliance with the Data Protection Act 1998 and the Human Rights Act 1998. PS has provided evidence of their participation in the Pan-Lothian and Borders Partnership General Protocol for Sharing Information (Evidence 14.1). This is a two-level partnership with councils and NHS bodies in the Lothian and Borders area with a general protocol supporting the creation of ISPs on more specific areas of information sharing. It is an example of an ISP involving a legacy police force but which is still operational after the creation of PS. Evidence 14.2, the Grampian Strategic GIRFEC Group Practitioners' Guide to Information Sharing, June 2014, which comprises a partnership between PS, NHS Grampian and councils in the Grampian area, provides staff with practical guidance in the operation of ISPs. Evidence 14.3 is an example of a specific ISP entered into with the Scottish Criminal Cases Review Commission, detailing each party’s obligations with regards to the information being shared.

	🟩	🟩	The link to the PS Information Charter on their website explains to the public how their information may be shared. The PS Corporate Strategy, 2014 (Evidence 11.1, page 67) highlights PS's commitment to improving information sharing processes. PS are currently developing a toolkit to assist Divisions in reviewing and revising their current procedures. This is scheduled for completion at the end of December 2014, with subsequent training being rolled out in January 2015. The Keeper commends this approach. Revised ISPs will be published on PS's intranet with details on who is responsible for them and when they are due for review. The Keeper agrees that PS have robust procedures in place for enabling the secure sharing of information with other bodies.

6. Keeper's Summary

Elements 1-14 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.

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

Robert Fotheringham
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.

Tim Ellis

……………………………………………

Tim Ellis
Keeper of the Records of Scotland