

Public Records (Scotland) Act 2011

Scottish Information Commissioner Assessment Report

The Keeper of the Records of Scotland

30 April 2014

Contents

1. Public Records (Scotland) Act 2011	2
2. Executive Summary	3
3. Authority Background	4
4. Assessment Process	5
5. Model Plan Elements: Checklist	5
6. Keeper's Summary	14
7. Keeper's Determination	15
8. Keeper's Endorsement	16

1. Public Records (Scotland) Act 2011

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

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

legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

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

2. Executive Summary

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

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

3. Authority Background

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

The Freedom of Information (Scotland) Act 2002

The Environmental Information (Scotland) Regulations 2004
The INSPIRE (Scotland) Regulations 2009

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

<http://www.itspublicknowledge.info/home/ScottishInformationCommissioner.aspx>

4. Keeper's Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether the Scottish Information Commissioner 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 <i>Compulsory element</i>	G	G	<p>The submitted records management plan (RMP) of the Scottish Information Commissioner (OSIC) identifies Rosemary Agnew, the Scottish Information Commissioner as the individual who is responsible for management of the authority’s public records.</p> <p>The OSIC <i>Information and Records Management Policy</i> document (submitted to the Keeper as evidence 3) confirms that the overall responsibility for records management falls to the Commissioner (paragraph 17).</p> <p>The operational efficiency of OSIC systems including information management is routinely reported to the Commissioner under procedures set out in a <i>Governance Reporting Arrangements</i> document that has been provided to the Keeper (evidence 9).</p> <p>As it is the Commissioner herself, rather than her office, that appears in the schedule to the Public Records (Scotland) Act 2011, the Keeper agrees that Ms Agnew is an entirely appropriate individual to adopt this role.</p>
2. Records Manager <i>Compulsory element</i>	G	G	<p>The RMP identifies David Lowrie, Head of Operational Management at OSIC as the individual who is responsible for ensuring compliance with the plan.</p> <p>The OSIC <i>Information and Records Management Policy</i> document (evidence 3) confirms that the Information Commissioner has delegated day-to-day records management responsibilities to OSIC’s Head of Operational Management.</p>

			<p>The OSIC <i>Information and Records Management Handbook</i>, which provides guidance to OSIC staff in support of the <i>Information and Records Management Policy</i>, explains the required competencies for this post (section 8). The Keeper agrees these competencies are appropriate for the individual with operational records management responsibility.</p> <p>The <i>Handbook</i> also specifically charges the Head of Operational management with the secure destruction of hardware (paragraphs 171 and 172).</p> <p>The Keeper agrees that an appropriate individual has been appointed to implement the RMP.</p>
<p>3. Policy Compulsory element</p>	<p>G</p>	<p>G</p>	<p>The Scottish Information Commissioner has supplied the Keeper with her <i>Information and Records Management Policy</i> v01.08 approved by the Senior Management Team in August 2013 and the supporting staff guidance <i>Information and Records Management Handbook</i> v02.02 approved by the Senior Management Team January 2014.</p> <p>The <i>Policy</i> (submitted as evidence 3) explains the importance of records management for the business of the Scottish Information Commissioner. It refers to staff training, information security and details the reporting structure for records management issues in the organisation. It also explains the legal framework under which OSIC's records are managed.</p> <p>The <i>Handbook</i> (submitted as evidence 4) is available to all staff, including contractors and other thirds parties who have access to OSIC's business systems. It explains what is expected of staff in the creation, naming and storage of records including e-mail. Section 7 deals with record disposal.</p> <p>(See <i>Handbook</i> under General Comments above)</p> <p>The Keeper agrees that the Scottish Information Commissioner has an appropriate records management policy in place and that it is strongly supported by staff guidance.</p>

<p>4. Business Classification</p>	<p>G</p>	<p>G</p>	<p>OSIC operate a functional file plan referred to in the <i>Information and Records Management Policy</i>. The file plan and retention schedule, which are a single document, have been provided to the Keeper (evidence 5).</p> <p>The file plan covers the full business of the Scottish Information Commissioner.</p> <p>The SIC holds public records on a suite of systems depending on business use. For example case files are held on Workpro, corporate records on INVU or a structured drive, staff files on a new system called 'Simply Personnel' etc. Paper submissions relating to cases are scanned into the electronic systems and the originals destroyed or added to hard copy files. The principle file is the file in the electronic system and the paper file a working copy. The Keeper is satisfied that OSIC properly controls the use of these systems.</p> <p>The <i>Investigations Procedures</i> (extract supplied to Keeper with evidence 2) document explains to staff the functionality of the systems.</p> <p>Section iii of the <i>File Plan and Retention Schedule</i> document refers to the annual review of the plan and schedule and the reporting of such a review to the Senior Management Team. As the file plan is central to the whole of OSIC's records management provision the Keeper commends the regular supervised review of its effectiveness.</p> <p>OSIC records management documents and guidance are available to staff on the INVU system.</p> <p>It is not thought that any <u>Function</u> of the Scottish Information Commissioner is contracted out to a third party.</p> <p>The Keeper agrees that the Scottish Information Commissioner has a business classification system that covers the entire operation of the authority.</p>
-----------------------------------	-----------------	-----------------	--

5. Retention schedule	G	G	<p>OSIC operate a full retention schedule matched against the file plan (see element 4 above) and appearing with it as part of a single document. The retention schedule is referred to in the <i>Information and Records Management Policy</i>.</p> <p>The Keeper agrees that the Scottish Information Commissioner has a retention schedule that covers the entire operation of the authority and matches the business classification scheme (it is, in fact, part of that scheme)</p>
6. Destruction Arrangements <i>Compulsory element</i>	G	G	<p>Electronic Records: A step by step guide to the destruction of electronic records in the various systems in which they are held, is provided to staff in the document <i>Records Review Procedures</i> (v01.02 dated 31/01/14) which has been provided to the Keeper (evidence 6). This document provides useful flowcharts for staff.</p> <p>The destruction of electronic copies created during the scanning process is specifically dealt with in the <i>Investigation Procedures</i> document – see 13.12 (extract provided to Keeper in evidence 2)</p> <p>A sample page from a destruction log has been provided as evidence that the procedures are in operation.</p> <p>Paper Records: OSIC have a contract with Shred-it to carry out the secure, onsite, irretrievable destruction of paper records. A sample of a destruction certificate issued by Shred-it has been provided to the Keeper as evidence that this contract is operational (evidence 2 6.1).</p> <p>A sample page from a paper destruction log has been provided as evidence that the procedures are in operation.</p>

			<p>Hardware: The OSIC <i>Information and Records Management Handbook</i>, which provides guidance to OSIC staff in support of the <i>Information and Records Management Policy</i>, specifically charges the Head of Operational management with the secure destruction of hardware (paragraphs 171 and 172). Details of how this is accomplished are included in the <i>Handbook</i>.</p> <p>A sample of a destruction certificate issued by Restructa has been provided to the Keeper as evidence that a contract is operational for the destruction of IT equipment (evidence 2 8.6).</p> <p>Back-Ups: Back-up tapes are overwritten on weekly cycle (Monday to Monday, Tuesday to Tuesday etc.). Back-ups used by the IT support provider as part of the recovery provision are returned and overwritten as part of the normal cycle.</p> <p>The <i>Handbook</i> is available to all staff, including contractors and other thirds parties who have access to OSIC’s business systems. It explains what is expected of staff in the creation, naming and storage of records including e-mail. Section 7 deals with record disposal.</p> <p>Destruction of records appears as section 2 of the <i>File Plan</i>.</p> <p>OSIC operate a <i>Destruction Register</i> to record the metadata of electronic records that have been destroyed. There is also a high level <i>Confidential Destruction Register</i> (access limited to key staff).</p> <p>The Keeper agrees that the Scottish Information Commissioner has properly considered the irretrievable destruction of her records.</p>
7. Archiving and Transfer <i>Compulsory element</i>	G	G	<p>The Scottish Information has a Memorandum of Understanding with the Keeper of the Records of Scotland for the deposit of records for permanent preservation in the National Records of Scotland.</p>

			<p>This is confirmed by a copy of the MOU sent in evidence and by the Keeper's Client Management Team.</p> <p>The Keeper therefore agrees that the Scottish Information Commissioner has proper provision in place for the archiving of her public records.</p>
8. Information Security Compulsory element	G	G	<p>OSIC does not have a single <i>Information Security Policy</i> that could be supplied to the Keeper. However, the protection of information assets both physically and intellectually is embedded in <i>Information and Records Management Policy</i> (for example Section 6), <i>Information and Records Management Handbook</i> (Section 4 uses of drives), <i>The Employee Handbook</i> (evidence 2 8.2 151 onwards), etc.</p> <p>OSIC have provided a copy of their <i>Risk Register</i> and <i>Clear Desk Policy</i> (which is part of the <i>Staff Manual</i>)</p> <p>The Keeper agrees that the Scottish Information Commissioner properly considers information security.</p>
9. Data Protection	G	G	<p>The Scottish Information Commissioner has a current Data Protection Policy, approved by the Senior Management Team on 28 January 2014. This has been supplied to the Keeper.</p> <p>The policy is available to the public from: http://www.itspublicknowledge.info/home/SICPublicationScheme/PSGuidetoInfo.aspx</p> <p>Furthermore, the principles of data protection are embedded throughout the rest of the evidence suite supplied to the Keeper such as the <i>Staff Manual</i> (evidence 2 8.2 173 for example)</p> <p>A section of the <i>Employee Handbook</i> (12.3 – submitted to the Keeper as an extract under evidence 2) is dedicated to explaining the Commissioner's responsibilities regarding sensitive personal information held about her staff.</p>

			<p>The Commissioner is registered with the Information Commissioner (reg. Z8091699).</p> <p>The Scottish Information Commissioner publishes subject access guidance at: http://www.itspublicknowledge.info/home/AboutSIC/RequestingInformationFromTheCommissioner.aspx</p> <p>The Keeper agrees that the Scottish Information Commissioner has properly recognised her responsibilities under the Data Protection Act.</p>
10. Business Continuity and Vital Records	G	G	<p>OSIC have a <i>Business Continuity Plan</i>. The contents list and day-to-day action plan have been provided to the Keeper. By these extracts, the plan would appear to detail a robust set of procedures.</p> <p>The Keeper agrees that the Scottish Information Commissioner has a business continuity plan that considers records.</p>
11. Audit trail	G	G	<p>OSIC holds public records on a suite of systems depending on business use. For example case files are held on Workpro, staff files on Simply Personnel etc. Each system has a clearly defined audit trail and, where not imposed automatically by the software, the Keeper has seen evidence of staff instructions regarding naming conventions and version control. For example: The <i>Information and Records Management Handbook</i> explains what is expected of staff in the creation, naming and storage of records including e-mail.</p> <p>The <i>Investigations Procedures</i> (extract supplied to Keeper with evidence 2) document explains to staff the functionality of the systems. At 13.6 the naming convention instruction for paper files are explained at 13.8 the same for electronic files in WorkPro.</p> <p><i>This Handbook</i> is available to all staff, including contractors and other thirds parties who have access to OSIC's business systems. Furthermore the importance of good records</p>

			<p>management is embedded in the <i>Staff Handbook</i>. The staff Handbook instructs staff to save corporate e-mails in the central systems rather than in the e-mail system (extract provided as evidence 2 8.2 – see 150 for e-mail management)</p> <p>The Keeper agrees that the Scottish Information Commissioner has procedures in place to track records and assure identification of the current version of these records.</p>
<p>12. Competency Framework for records management staff</p>	<p>G</p>	<p>G</p>	<p>The OSIC <i>Information and Records Management Handbook</i>, which provides guidance to OSIC staff in support of the <i>Information and Records Management Policy</i>, explains the required competencies for this post (section 8).</p> <p>The covering statement from the Information Commissioner (page 3 of the RMP) states ‘all staff maintain, and develop as necessary, their competence in information and records management’. The documents central to the operation of OSIC’s records management system, such as the <i>Information and Records Management Handbook</i> repeatedly support this statement regarding training.</p> <p>The Keeper agrees that the individual named in element two of the RMP has the required competencies for the role and that the Scottish Information Commissioner has properly considered appropriate training on information management for OSIC staff.</p>
<p>13. Assessment and Review</p>	<p>G</p>	<p>G</p>	<p>The covering statement from the Information Commissioner (page 3 of the RMP) commits OSIC to ‘routinely review and develop as necessary our policies, procedures and practices’</p> <p>The operational efficiency of OSIC systems including information management is routinely reported to the Scottish Information Commissioner under procedures set out in a <i>Governance Reporting Arrangements</i> document that has been provided to the Keeper (evidence 9).</p> <p>The procedure for the review of OSIC documents is set out in <i>Management and Review of</i></p>

			<p><i>Key Documents</i> (v01.03 supplied as evidence 10). Changes to key documents are logged in a Register which is itself reviewed annually by the senior management team. In the submitted <i>Employee Handbook</i> extract (evidence 2 8.2 147) there is an example of the Commissioner committing to make staff aware of any updated policies. The importance of staff being informed when changes are made to policies is an important issue and the Keeper acknowledges that OSIC is addressing it.</p> <p>Section iii of the <i>File Plan and Retention Schedule</i> document refers to the annual review of the plan and schedule and the reporting of such a review to the Senior Management Team. Any changes to the file plan have to gain approval at a senior level and there is a paper trail created showing those changes. As the file plan is central to the whole of OSIC's records management provision the Keeper commends the regular, supervised review of its effectiveness.</p> <p>The methodology of the annual review is set out in a document <i>Records Review Procedures</i> which has been provided to the Keeper (evidence 6).</p> <p>The Keeper agrees that the Scottish Information Commissioner has formal records management review procedures in place that are appropriate to the authority's business.</p>
14. Shared Information	G	G	<p>The Scottish Information Commissioner does not currently share records with third parties. Nor does she engage in record creation on a shared platform. However, the Keeper has been made aware of a commitment by OSIC that, should they undertake such work in the future, they will included clauses establishing records governance protocols in any data sharing agreements.</p>

General Notes on RMP, Including Concerns:

The Scottish Information Commissioner (SIC) RMP is accompanied by a letter from the SIC. She also includes a covering note to the plan itself (page 3) acknowledging the importance of records management to her office's operational efficiency.

Future Developments

In some places the submitted RMP includes suggestions for future improvements (such as element 11). The Keeper commends this and notes that such forward planning is entirely in the spirit of the Public Records (Scotland) Act 2011. He asks if he may be kept informed of any developments that materially affect the agreed plan.

Handbook

The Scottish Information Commissioner has supplied the Keeper with a copy of an *Information and Records Management Handbook* which offers guidance to OSIC staff. The Keeper commends this document and asks if he may share it with other public authorities. Although it is clearly designed for OSIC staff, the *Handbook* offers best practice guidance generally and is a high-quality example of how staff guidance might be arranged. If the Commissioner agrees, the Keeper would like to provide a PDF version as part of his online Guidance Document. Please be aware that this is a decision for the Commissioner alone; the Keeper will not publish any part of the submitted evidence package without her express approval.

6. Keeper's Summary

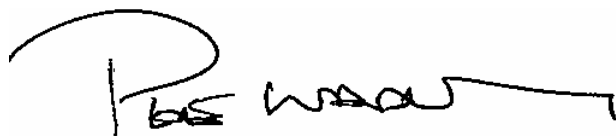
Elements **1 – 14** that the Keeper considers should be in a public authority records management plan have been properly considered by the Scottish Information Commissioner. Policies and governance structures are in place to implement the actions required by the plan.

7. Keeper's Determination

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

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

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



.....
Pete Wadley
Public Records Officer



.....
Robert Fotheringham
Public Records Officer

8. Endorsement of Report by the Keeper of the Records of Scotland

Either

The report has been examined and is endorsed under the signature of the Keeper of the Records of Scotland as proof of compliance under section 1 of the Public Records (Scotland) Act 2011, and confirms formal agreement by the Keeper of the RMP as submitted by the Scottish Information Commissioner. In agreeing this RMP, the Keeper expects the Scottish Information Commissioner to fully implement the agreed RMP and meet its obligations under the Act.



.....
Tim Ellis
Keeper of the Records of Scotland