Records management plan

The Scottish Parliamentary Corporate Body (SPCB)
The Scottish Parliament
The Scottish Commission for Public Audit (SCPA)
This updated Records management plan is presented to the Keeper of the Records of Scotland for the Keeper's agreement under section 1 of the Public Records (Scotland) Act 2011 and updates the plan presented in 2014.

The plan, prepared by the Scottish Parliamentary Corporate Body (SPCB), sets out proper arrangements for the management of public records created, managed and disposed of by the SPCB, the Scottish Parliament and the Scottish Commission for Public Audit.

The Keeper of the Records of Scotland will be notified of any changes made to this records management plan in accordance with section 5(6) of the Public Records (Scotland) Act 2011.
Introduction

The Scottish Parliament recognises that records management is vital for the proper functioning of any organisation and is essential in ensuring that the Scottish Parliament has accurate, reliable and accessible records of its work to support its business and maintain a sufficient archive of its activities.

This is an update to the Scottish Parliament's first records management plan following the implementation of a document and records management system. It sets out what has been done to improve the records management function in the Scottish Parliament and provides detail on what is planned to further enhance records management in compliance with the requirements of the Public Records (Scotland) Act 2011 (PRSA).

The records management plan has been prepared in accordance with statutory criteria set out in the PRSA, and having regard to the Keeper of the Records of Scotland’s model records management plan and guidance on the development of records management plans.

For clarity, all references to the Scottish Parliament in this plan include the Scottish Parliament, the Scottish Parliamentary Corporate Body and the Scottish Commission for Public Audit.

Plan structure

For each element, the plan reviews the Scottish Parliament’s current records management maturity, supported by evidence where necessary, with a summary of current maturity from the records management maturity model. In addition, each element contains information concerning planned activities to demonstrate how the Scottish Parliament plans to improve records management maturity.

The records management maturity model (updated evidence item 1) has been developed using JISC Info Net and used to plan records management good practice developments. The maturity model makes it possible to demonstrate progress and to identify gaps that need to be addressed.

The four levels of maturity are:

0 Absent – Shows no evidence of awareness of the need to take a strategic approach to the management of records;

1 Aware – Uncoordinated local attempts to improve records management in response to local issues;

2 Defined – Coordinated attempts to improve records management underway; and

3 Embedded – The effective management of records is fully integrated within strategic and operational activities.
Background

Records management is a strategic priority for the Scottish Parliament and a key activity in establishing the Parliament as an exemplar of good governance, excellent resource management and accountability (Strategic plan, updated evidence item 2).

The Scottish Parliament successfully implemented a corporate electronic document and records management system in 2016. Digital records are managed in this system according to corporate policies. Paper records are managed at box level and stored in either an internal storage facility, managed by information management staff or with our records storage contractor in an off-site storage facility.

Records management project (2007 to 2013)

A project to improve the records management capability of the Scottish Parliament was embarked upon in 2007. It was recognised that long-term commitment was required in order to improve records management. In recognition of the requirement to develop a robust records management culture, prior to consideration of any technological solution, the project adopted a phased approach.

- Phase 1 – Records management foundations (2007 to 2009)
- Phase 2 – Practical application of records management principles (2010 to 2012)
- Phase 3 – Defining scope of a records management system project (2012 to 2013)

Document and records management (DRM) project (2013 to 2016)

To build on the achievements of previous project phases, a project to identify, develop and implement a DRM system (SPShare) started in 2013 (evidence item 3) and ended in March 2016 (new evidence item 91).

The Project focussed on introducing agreed organisational policies and consistent processes on the DRM system for a combined document and records management approach. This was a significant change project for the organisation, moving from limited management of documents and records in any consistent, organised way to a more controlled and consistent approach that would involve more, rather than less, effort from staff.

The system implemented as the electronic document and records management solution to meet requirements was SharePoint 2013. To further enhance the functionality and capability of the software, the Automated Intelligence AI.Compliance Extender plugin was also implemented to complement the SharePoint platform. AI.Compliance Extender is built as an extension solution for SharePoint 2013 leveraging and extending SharePoint for information management and governance. It provides a robust
classification schema to extend the records management capability available in SharePoint 2013.

**Project outcomes**
The DRM project delivered the following core outputs:

- a technical infrastructure and support teams enabling a digital working environment;
- a blended training programme used to train staff on the use of SPShare and how to create, edit and manage documents and how to declare documents as records;
- a records centre to actively manage records in accordance to a functional file plan and retention schedule.

**Current and planned activities**

**Document retention policy and good practice project (2016 - 2018)**

The Document retention policy and good practice project will implement the document retention policy (contained within the Records management policy, updated evidence item 8) requiring all records owners to routinely and regularly declare documents. Once implemented, the policy will enable the deletion of all documents not declared as records or modified within the previous 24 months. This project is a key follow on action from the DRM project to encourage the routine declaration of records, to enhance the reliability of the records centre and is seen as crucial to the on-going success of SPShare. The project will also improve the search capability of SPShare by removing ephemera and will help address the feedback around search captured during the DRM project.
Element 1 – Senior management responsibility

The senior post-holder with overall responsibility for the records management plan is:

Alan Balharrie  
Group Head of Digital Services Group  
The Scottish Parliamentary Corporate Body  
The Scottish Parliament  
Edinburgh  
EH99 1SP

A statement of responsibility (updated evidence item 6) is supplied with the records management plan to confirm that Alan Balharrie endorses the Scottish Parliament’s records management policy.

Records management has the full support of the SPCB and the Parliament’s senior managers, demonstrated by the strategic plan (updated evidence item 2), which commits the SPS to establishing the Parliament as an exemplar of good governance, excellent resource management and accountability.

Primary evidence in support of plan

Updated item 6 Statement of responsibility for records management  
Updated item 8 Records management policy

Secondary evidence in support of plan

Updated item 1 Records management maturity model  
Updated item 2 Strategic plan 2017  

Maturity model (A1) – Organisational arrangements to support records management

Records management is recognised as a core corporate function with defined roles and responsibilities at both a strategic and operational level.

Current level of maturity – 3 - Embedded
Element 2 – Records Manager responsibility

The post-holder with responsibility for ensuring that the Scottish Parliament complies with the plan is:

Gordon Hobbs
Information Manager
The Scottish Parliamentary Corporate Body
The Scottish Parliament
Edinburgh
EH99 1SP

Gordon Hobbs has overall day-to-day responsibility for records management and the implementation of the Scottish Parliament’s records management plan. Updated evidence item 6 confirms that Gordon Hobbs is the person responsible for implementing the Records management plan. Roles and responsibilities are further defined in the Scottish Parliament’s Records management policy (updated evidence item 8).

<table>
<thead>
<tr>
<th>Primary evidence in support of plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated item 6 Statement of responsibility for records management</td>
</tr>
<tr>
<td>Updated item 8 Records management policy</td>
</tr>
<tr>
<td>Item 73 Information Manager job vacancy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary evidence in support of plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated item 1 Records management maturity model</td>
</tr>
<tr>
<td>Updated item 9 Records management strategy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maturity model (A6) – Organisational arrangements to support records management</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SPCB should have a qualified records manager in post and a community of records management champions. Records management staff are given opportunities for professional development.</td>
</tr>
</tbody>
</table>

**Current level of maturity** – 3 - Embedded
Element 3 – Records management policy statement

Records management is recognised as being essential in ensuring that the Scottish Parliament has accurate, reliable and accessible records of its activities, to support its business and to maintain a sufficient archive of its activities.

The Scottish Parliament Records management strategy (updated evidence item 9) and Policy (updated evidence item 8) were endorsed by the Leadership Group in January 2017 (new evidence item 85).

In support of the Strategy and Policy, Records management procedures and guidance (updated evidence item 12) has been developed and implemented to ensure that staff have the necessary information available to allow them to apply the Policy and Strategy consistently to all information the Scottish Parliament creates, receives and shares. Records management procedures were updated following implementation of the DRM system and SPShare-specific training material (new evidence items 86-89) developed to provide information on SPShare features and to demonstrate how to use the system itself. The strategy, policy and Procedures documents are published on the records management pages of the Scottish Parliament’s intranet and available on SPShare. SPShare training material (evidence items 86 to 89) complements the Records management procedures and is available on SPShare, on the dedicated http://help site, and through the Parliament’s social personalised learning system, SPLearning.

In recognition of what is required in order to operate an effective records management system that embraces records in all formats, the DRM system embeds controlled metadata in all records. The metadata of disposed records is maintained permanently in the file plan location where the original record was located. The Scottish Parliament metadata standard (evidence item 13), which is based on the e-Government metadata standard and Dublin Core, defines and controls the use of metadata in new Scottish Parliament electronic systems.

Primary evidence in support of plan
Updated item 8 Records management policy
Updated item 9 Records management strategy
Item 10 Operational Management Group minutes, May 2010
Item 11 Leadership Group signoff of the records management policy and strategy
Item 84 RM intranet homepage
New item 85 Leadership Group minutes and paper, January 2014

Secondary evidence in support of plan
Updated item 1 Records management maturity model
Updated item 12 Records management procedures and guidance
Item 13 Scottish Parliament metadata standard
New item 86 SPShare training material – InfoPods
New item 87 SPShare training material – Quick reference guides
New item 88 SPShare training material – session slides
New item 89 SPShare training material – session plan

Maturity model (B) – Records management policy

B1 The SPCB will issue a policy covering records management. This should be endorsed by the Clerk/Chief Executive and be readily available via the intranet.

Current level of maturity – 3 – Embedded

B2 The policy should be kept up-to-date so that it reflects the current needs of the SPCB.

Current level of maturity – 3 - Embedded
Element 4 – Business classification

The Scottish Parliament file plan (updated evidence item 17) was developed and implemented during the DRM project. The file plan was developed following workshops involving staff from across the Scottish Parliament. Staff attending workshops identified the organisation’s core functions, component activities and associated transactions in order to develop the core structure of the file plan. The file plan was reviewed throughout the DRM project and adjusted in response to business needs when required. No fundamental amendments were made following completion of the DRM project.

The file plan is now actively used in the DRM system’s records centre, the central repository for all records managed in the system. The DRM system provides, within the records centre, the class-folder file plan structure that represents business functions, activities and transactions. Records are associated with a class and will therefore maintain a definitive business context that will continue to link the record with the business process that generated it.

**Primary evidence in support of plan**
- Item 14 File plan workshops participant role
- Item 15 File plan workshops presentation
- Item 16 File plan workshops – summary of outcomes
- Updated item 17 File plan

**Secondary evidence in support of plan**
- Updated item 1 Records management maturity model

**Maturity model (D1) – Records systems**

Records systems should enable the context of each record and its relationship to other records to be understood through classification in a file plan and for groups of like records to be managed together.

**Current level of maturity** – 3 – Embedded (updated)
Element 5 – Retention schedule

A records retention schedule was delivered in phase 1 of the records management project following an information audit. The Information Manager worked with business areas to identify record types created by the organisation as well as their recommended retention period, in accordance with statutory, legislative and business requirements. The retention schedule was signed off by each Office Head, the Office for the Solicitor of the Scottish Parliament and was made available to the NRS for comment to ensure that our obligations to preserve records with the NRS were reflected appropriately. This retention schedule was implemented during records reviewing activities in phases 1 and 2 of the records management project. The retention schedule (evidence item 18) was last updated in phase 2 of the records management project and will be reviewed during the Document retention policy and good practice project to reflect DRM project developments and to ensure it reflects the file plan. The retention schedule is applied to records in all formats.

In addition to the records retention schedule, the Scottish Parliament has records management procedures and guidance, offering practical guidance to staff on the creation, use, management and disposal of records. The procedures and guidance describe how the Scottish Parliament creates and manages records and details procedures we follow to ensure records are reviewed according to central guidance and routinely and securely disposed of.

Records retention rules are applied to the file plan automatically which then enables the application of retention rules based on pre-defined criteria e.g. location, file type etc. The system also prompts information management staff on the need to review records using pre-defined metadata.

Primary evidence in support of plan
Item 18 SPCB records retention schedule
Updated item 12 Records management procedures and guidance

Secondary evidence in support of plan
Updated item 1 Records management maturity model

Maturity model (G1, G3, G4) – Disposal of records
G1 Records should not be kept after they have ceased to be of use to the SPCB unless they are known to be the subject of litigation or a request for information; or they have long-term value for historical or other research purposes.

Current level of maturity – 3 – Embedded (updated)
G3 Retention schedules should contain sufficient details about the records to enable the records to be easily identified and the disposal action applied to them on a routine and timely basis. Retention schedules should be kept up to date. Retention schedules and disposal decisions should be implemented by properly authorised staff and should take account of variations caused by, for example, outstanding requests for information or litigation.

Current level of maturity – 3 - Embedded

G4 If any records are not included in retention schedules, arrangements should be made to review them and decide whether they can be destroyed or should be selected for permanent preservation.

Current level of maturity – 3 – Embedded

Planned activity 5.1 – Updating retention schedule

The retention schedule will be reviewed during the Document retention policy and good practice project to reflect current and previous project developments and to mirror the file plan.

Planned activity 5.4 – Centralisation of records

A business-as-usual activity has been scoped, and will be implemented following the Document retention and good practice project, to store and manage hardcopy vital records in a controlled and audited environment managed by Information Management staff.
Element 6 – Destruction arrangements

Hardcopy records

The Scottish Parliament has robust and auditable disposal arrangements for paper records stored on-site or in off-site commercial storage. Hardcopy documents and records of a sensitive nature not managed off-site are destroyed on-site using a confidential shredding service (evidence item 19). The contractor provides a confidential destruction and recycling service in compliance with EN15713:2009. A certificate of destruction (evidence item 20) is provided for each destruction actioned by the contractor. In addition, an internal log book (evidence item 21) is maintained to ensure an audit trail captures the movement of confidential waste up to the point of transfer to the contractor for disposition. In addition to the detail provided by the confidential shredding service, information owners using this service must also log the destruction of records using an electronic form (evidence item 22) available to all staff and contractors on the intranet.

Hardcopy non-current records that need to be kept for a pre-determined period are sent to an off-site storage contractor. Records destroyed by the off-site storage contractor are shredded, pulped and recycled with a destruction certificate issued within 48 hours and a permanent log of destroyed records is kept indefinitely and can be viewed on a web based inventory tool (evidence item 24).

Digital records

Records managed in the DRM system are destroyed using the AI.Compliance Extender plugin disposition workflow. The AI.Compliance Extender plugin has extended the disposal functionality of SharePoint 2013 by implementing the concept of ‘disposal stubs’ whereby record content is destroyed, but a metadata stub is retained indicating that a record once existed in that location. All metadata for the disposed record is maintained within the file plan. All disposal actions within the DRM system are fully audited and limited to information management staff. In addition to the standard metadata (please see Metadata standard, evidence item 13) the following metadata is captured during the records reviewing and disposition process:

- Retention schedule ID
- Retention period
- Disposal trigger
- Disposal action
- Disposal date
- Date of last review
- Disposal reviewer details
- Disposal review details
- Disposal authorised by
- Disposal comment
**Primary evidence in support of plan**
Item 19 Recycling and waste management services contract extract
Item 20 Recycling and waste management services destruction certificate
Item 21 Recycling and waste management services log book extract
Item 22 Records destruction form (small-scale)
Item 23 Records destruction guidance
Item 24 Off-site records and media tape storage contract
Item 25 Off-site records storage destruction certificate
Item 80 Recycling and disposal of IT equipment contract extract
Item 81 Recycling and disposal of IT equipment - Disposal list template
Item 82 Recycling and disposal of IT equipment - Disposal collection template
Item 83 Recycling and disposal of IT equipment - Disposal confirmation extract

**Secondary evidence in support of plan**
Updated item 1 Records management maturity model
Updated item 12 Records management procedures and guidance
Item 18 SPCB records retention schedule

---

**Maturity model (D3 & D4) – Records systems**

D3 Records systems should be documented to facilitate staff training, maintenance of the system and its reconstruction in the event of an emergency.

**Current level of maturity** – 2 - Defined

D4 Record systems should enable the closure of folders, files and similar records at an appropriate time according to the specific nature and function of the records in question and should be supported by processes designed to identify and act upon such triggers for closure.

**Current level of maturity** – 3 – Embedded (updated)

**Maturity model (G2, G5 & G6) – Disposal of records**

G2 Disposal of records should be undertaken only in accordance with clearly established policies including: a) an overall policy, stating in broad terms the types of records likely to be selected for permanent preservation; and b) retention schedules which identify and describe records to which a pre-defined disposal action can be applied.

**Current level of maturity** – 3 - Embedded
G5 All copies of records scheduled for destruction should be destroyed in as secure a manner as required by the level of confidentiality or security markings they bear, regardless of whether destruction is carried out ‘in house’ or by external contractor.

**Current level of maturity** – 3 – Embedded (updated)

G6 Details of destruction of records should be kept, either as part of the audit trail metadata or separately.

**Current level of maturity** – 3 – Embedded (updated)

---

**Planned activity 6.2 Irrevocable deletion**

The DRM system ensures the irrevocable deletion of records in the system. This process will be documented to aid maintenance and training.

**Planned activity 6.3 Paper disposition recording process**

Disposition recording process to be improved and implemented for paper records held in central repository. The possibility of managing hardcopy records in the DRM system file plan, including destruction arrangements and the logging of destruction in the electronic environment will be investigated.
Element 7 – Archiving and transfer arrangements

The Scottish Parliament has in place an arrangement to dispose records of archival value with the NRS. The NRS and the Parliament are guided by a Memorandum of Understanding (evidence item 26) and the NRS had an opportunity to contribute to the SPCB records retention schedule which identifies the records selected for permanent preservation. The Records management procedures and guidance (updated evidence item 12) details the process for transferring records identified by the retention schedule for permanent preservation with the NRS.

In order to facilitate export and/or transfer of records from the DRM system, the AI.Compliance Extender plugin has an Import – Export module which imports and exports both SharePoint content and metadata in a number of XML formats allowing transfer to the NRS and within and between other organisations and systems as required. With the export, entire hierarchical structures or flat search results can be exported. These features allow reorganisations and exports to take place without impacting the integrity of records.

**Primary evidence in support of plan**
- Item 26 Memorandum of understanding between the Scottish Parliament and the NRS
- Item 27 NRS transfer form

**Secondary evidence in support of plan**
- Updated item 12 Records management procedures and guidance
- Item 18 SPCB records retention schedule

**Maturity model (G7) – Disposal of records**

Records selected for permanent preservation and no longer required by the SPCB will be transferred to the National Records of Scotland.

**Current level of maturity** – 3 - Embedded

**Planned activity 7.1 Transfer of digital records to the NRS**
The DRM system enables the transfer of digital records in a MoReq compliant format. The system therefore allows for the transfer of all records within it as well as their associated metadata to be exported to another system in a standard, re-usable format. Arrangements will be made with the NRS to explore the process of transferring digital records to the NRS.

**Planned activity 7.2 Revised guidance**

Existing guidance on identifying records of historical, cultural and research value will be reviewed and enhanced to ensure that revised working practices and storage methods are reflected in guidance.
Element 8 – Information security

The Scottish Parliament has a number of well-established policies and procedures concerning the security of its information. The information security policy (evidence item 28) covers information, data, software, hardware and communication networks for which the Business Information Technology (BIT) office is the custodian.

The Scottish Parliament protective marking system (updated evidence item 32) provides a layer of security for information contained within documents and records. Protective marking is the method by which the originator of information indicates to others the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the Parliament and its ultimate method of disposal.

The purpose of the system is to ensure that the Scottish Parliament’s information assets:

- are marked and secured correctly
- are protected from inappropriate or unauthorised access, amendment or disposition

An updated protective marking system was agreed by the Leadership Group in January 2017 (new evidence item 85) to reflect developments and new requirements following the successful implementation of SPShare during the DRM project.

The DRM system allows for the secure, audited storage of all electronic documents and records and enforces technological restrictions to prevent unauthorised access, destruction, alteration or removal of records.

---

**Primary evidence in support of plan**

- Item 28 Information security policy
- Item 29 Information security guide
- Item 30 Off network data handling
- Item 31 Leadership Group (2012) paper 081 – Business IT guidance: Off-network data handling
- Updated item 32 Protective marking system
- Item 33 Leadership Group minutes January 2014
- Item 34 Security incident reporting form
- Item 35 Security access arrangements for network shared drives
- Item 36 Process for creating network shares
- Item 37 Email for checking permission to be granted
Item 38 Password protection and encryption  
Item 39 Assyst knowledge base procedures  
Item 40 Encryption guidance  
Item 41 Server build  
Item 42 Protection of servers and electronic data  
Item 43 Description of electronic backups arrangements  
Item 44 Security manuals  
Item 45 Performance and capacity management report  
Item 46 Account audit  
Item 47 Routine information security reports  
Item 48 Data protection framework, including: policy on data sharing and policy on management of data breaches  
New item 85 Leadership Group minutes January 2017

Maturity model (D2) – Records systems  
Record systems should provide secure storage to the level of protection required by the nature, contents and value of the information in them and should protect records in digital systems from accidental or unauthorised alteration, copying, movement or deletion.

Current level of maturity – 3 – Embedded (updated)

Maturity model (E2) – Storage and maintenance of records  
Storage facilities for records should provide protection to the level required by the nature, contents and value of the information in them and be appropriate for their level of use.

Current level of maturity – 3 – Embedded (updated)

Maturity model (F1 & F2) – Security and access

F1 The SPCB will ensure that their storage arrangements, handling procedures and arrangements for transmission of records (particularly outside of the SPCB’s premises) reflect accepted standards and good practice in information security.

Current level of maturity – 3 – Embedded (updated)

F2 Access restrictions should be applied when necessary to protect the information concerned and should be kept up to date with external access being provided in accordance with relevant legislation.
Element 9 – Data protection

The Scottish Parliament has a legal obligation to comply with the requirements of the Data Protection Act 1998, ensuring that it has arrangements in place to manage, process and protect personal data. The Scottish Parliament’s data protection policy (evidence item 48) demonstrates the organisation’s commitment to compliance with the Act and the safeguarding and fair processing of all personal data held.

The Head of Information Governance is responsible for delivering expertise, advice, guidance and training on all aspects of information governance including data protection. The Head of Information Governance takes the lead in ensuring the Scottish Parliament is fulfilling its requirements under the Act.

The guide to submitting subject access requests to the Scottish Parliament is available on the Scottish Parliament website (evidence item 50). The Scottish Parliament is registered with the Information Commissioner as required by the Data Protection Act 1998, registration number Z7477607.

The Information management and governance team has responsibility for overseeing access restrictions to documents and records within the DRM system, ensuring compliance with the Protective marking system. The management of individual security groups required for the proper functioning of protective marking and DRM system security controls are devolved to business areas and individual owners. Changes cannot be made to security groups without the audited consent of group owners.

Primary evidence in support of plan

- Item 48 Data protection framework, including: Data protection policy, policy on managing the rights of data subjects, policy on data sharing and policy on management of data breaches
- Item 33 Leadership Group minutes January 2014
- Item 49 Data protection guidance
- Item 50 Subject access request guidance
- Item 51 Guidance on processing subject access requests
- Item 52 Subject access checklist
- Item 53 Personal data breach plan and guidance
- Item 54 Privacy impact assessments
- Item 55 Privacy impact assessment - project guidance
- Item 56 Privacy impact assessment template
- Item 57 Data protection training
Supporting evidence in support of plan

Item 28 Information security policy
Updated item 32 Protective marking system
Item 58 Data sharing guidance
Item 59 Data sharing checklist

Maturity model (E2) – Storage and maintenance of records
Storage facilities for records should provide protection to the level required by the nature, contents and value of the information in them and be appropriate for their level of use.

**Current level of maturity** – 3 – Embedded (updated)

Maturity model (F2) – Security and access
Access restrictions should be applied when necessary to protect the information concerned and should be kept up to date with external access being provided in accordance with relevant legislation.

**Current level of maturity** – 3 – Embedded (updated)

Planned activity 9.1 Digital records centre
An audit will be carried out to ensure that as many digital records are managed in the DRM system as possible.
Element 10 – Business continuity and vital records

The Scottish Parliament has Business Continuity plans for each office and a team structure in place to ensure that critical business can resume after an incident, emergency or disaster, in line with the Business Continuity strategy (evidence item 56) approved by the SPCB (evidence item 61). Plans detail the processes undertaken by each office, the resources used in those processes and the outputs resulting from successful completion of those processes; they also indicate the relative urgency of each activity to assist with prioritisation. Plans are reviewed annually and completely refreshed after each Scottish Parliament election.

A general salvage plan (evidence item 66), detailing physical items needed for resumption of critical business, was developed in 2012. A heritage salvage plan was developed in 2015 and applies to the art collection, Dewar collection, exhibitions and gifts collection. This plan will be used as a template for the development of a vital records salvage plan.

Business continuity and salvage plans show that the information resources required by offices to maintain business are almost wholly electronic. Back up of electronic storage is maintained in the following ways:

- Within the Parliament building electronic information is stored centrally on a Storage Area Network (SAN) which is synchronised almost instantaneously to another SAN in a separate part of the building.
- Data on the SAN is also synchronised to an external site at secure premises and data on that SAN is no more than 4 hours old.
- Data is also backed up to tape every night and moved each day to storage off-site with a specialist contractor (evidence item 24). Data from the tape backups can be restored internally or at the external site.

An exercise to identify vital records was undertaken in 2011 (evidence item 69) during phase two of the records management project. It was identified that existing IT disaster recovery procedures covered the management of records held electronically, no further investigation of electronic vital records was made at that point. Recommendations were made to improve the management of hardcopy vital records which are being implemented as a business as usual activity.

Primary evidence in support of plan

Item 61 SPCB (2011) Paper 060 Minutes
Item 63 LG (2013) Paper 066 – further development of BC plans unpublished
Item 64 Blank template – Office BC plan
Item 65 Internal audit paper AAB unpublished
Item 66 BCAP paper 07/4 Sep 2012 – salvage plan
Item 67 BCAP minutes
Item 69 Vital records – recommendations

Secondary evidence in support of plan
Item 24 Off-site records and media tape storage contract

Maturity model (E4, E5 & E6) – Storage and maintenance of records

E4 Records should remain usable for as long as they are required. The SPCB should put in place a strategy for the continued maintenance of records stored in digital systems and regularly inspect vulnerable paper files (e.g. early photocopies).

Current level of maturity – 1 - Aware

E5 Business continuity plans should identify and safeguard records considered vital to the organisation and backup copies of records in digital systems should be kept and stored securely in a separate location.

Current level of maturity – 2 - Defined

E6 Metadata for records in any format should be kept in such a way that it remains reliable and accessible for as long as it is required, which will be at least for the life of the records.

Current level of maturity – 3 – Embedded (updated)

Planned activity 10.1 Technological obsolescence of vital records
Implement vital records recommendations from phase 2 of the records management project. Also carry out an activity to assess the technological obsolescence of vital records held in the DRM system to ensure that it is known which, if any, digital records are at risk. In consultation with BIT, a plan for their preservation will also be developed as part of a comprehensive preservation strategy.
**Planned activity 10.2 Vital records plan**
An activity to identify and select electronic vital records held in the DRM system will be scoped and initiated. A plan for the management of vital records and their ongoing identification will be developed.

**Planned activity 10.3 Salvage plan**
Update salvage plan to include vital records.

**Planned activity (new) 10.4 Refine disaster recovery processes for SPShare**
Now that SPShare is embedded, an activity will be scoped to document the disaster recovery arrangements in place specifically for the new DRM environment.
Element 11 – Audit trail

Paper records

Non-current hard copy records are held in secure storage either in a secure on-site store or off-site with a records storage provider. The Scottish Parliament has records retrieval procedures for paper records held in storage (at box level). Records held in on-site or off-site storage are tracked using a database that is managed by information management staff (evidence item 70). There are electronic and paper trails for all transactions relating to receipt, transfer, return and disposal of records held in storage.

The DRM system offers the opportunity to manage paper records in the electronic sphere by using SharePoint’s external item feature. This enables the tracking of paper records in a digital environment, alongside digital records. This opportunity will be explored further in planned activities.

Digital records

Changes to documents in document repositories and all actions in the Records Centre file plan are audited (evidence item 72). The following auditing reports are available in the DRM system:

Content Activity Reports
- Content viewing
  This report shows all events where a user viewed content in a site.
- Content modifications
  This report shows all events that modified content in a site.
- Deletion
  This report shows all events that caused content in a site to be deleted or restored from the Recycle Bin.
- Content type and list modifications
  This report shows all events that modified content types and lists in a site.

Information Management Policy Reports
- Policy modifications
  This report shows all events related to the creation and use of information management policies on content in a site.
- Expiration and Disposition
  This report shows all events related to the expiration and disposition of content in a site.
Security And Site Settings Reports

Auditing settings
This report shows all events that change the auditing settings of Microsoft SharePoint Foundation.

Security settings
This report shows all events that change the security configuration of Microsoft SharePoint Foundation.

Custom Reports

Run a custom report
Manually specify the filters for Audit Reports.

Primary evidence in support of plan
Updated item 12 Records management procedures and guidance
Item 70 Hardcopy records storage inventory
Item 71 Hardcopy records storage retrieval tracking
Item 72 DRM system audit settings

Secondary evidence in support of plan
Item 36 Process for creating network shares
Item 37 Email for checking permission to be granted

Maturity model (E3) – Storage and maintenance of records
The whereabouts of records and who accesses them should be known at all times.

Current level of maturity – 3 – Embedded (updated)

Planned activities 11.2 External items
Investigate the implementation of external items in the DRM system to enable paper records to be managed in the file plan in an audited environment. In addition, and in parallel, a complete audit trail of paper records will be carried out with the intention to enable the use of external items and to allow for the management of paper vital records in a central records registry, managed by information management staff.
Element 12 – Competency framework for records management staff

The job specification (evidence item 73) for the Scottish Parliament's Information Manager role includes appropriate technical skills as identified in the FOISA code of practice on records management. The Scottish Parliament’s performance management system’s personal development plan (evidence item 76) ensures that the Information Manager receives appropriate on-going training in order to fulfil the requirements of the role. Performance management objectives relate directly to one of the strategic objectives set out in the organisation’s strategic plan (updated evidence item 2) or to an activity contained in the business area’s group or office plan (which in themselves will support the delivery of the strategic plan). Objectives cover all the key elements of job roles.

Site owners are nominated by their office and are expected to provide initial support and advice to colleagues within their own office and to provide an essential point of contact between the Information Manager and office staff. All site owners receive training from the Information Manager (evidence items 78 and 79).

**Primary evidence in support of plan**

Updated item 06 Statement of responsibility for records management
Item 73 Information manager job vacancy
Item 74 Performance management template (with relevant skills and behaviours for the Information Manager selected)
Item 75 Performance management system
Item 76 Professional development plan template
Item 77 Professional development plan guidance
Item 78 Champion training plan
Item 79 Champion training programme

**Secondary evidence in support of plan**

Updated item 1 Records management maturity model

**Maturity model (A6) – Organisational arrangements to support records management**

The SPCB should have a qualified records manager in post, a community of records management champions. RM staff given opportunities for professional
Records management plan – 2016

Development.

Current level of maturity – 3 - Embedded

Planned activity 12.1 Staff training
SPShare training has been developed and delivered. A permanent records management training programme will be developed to establish business-as-usual continuous training.

Planned activity 12.2 (new) Performance management
The Scottish Parliament’s performance management system is currently being redeveloped. Element 12 and supporting evidence will be updated to reflect performance management changes.
Element 13 – Assessment and review

This records management plan will be reviewed in accordance with the Keeper’s requirements. Periodic review of the records management function will employ the records management maturity model (updated evidence item 1).

Following closure of the DRM project, records management maturity was assessed using the maturity model (updated evidence item 1). Initial key performance indicators (KPIs) relating to the implementation of the document retention policy were also established (new evidence item 90). These initial KPIs are intended to inform Leadership Group of the progress being made by offices to adhere to the document retention policy and, in doing so, declaring records as business-as-usual. Following implementation of the document retention policy, a review of KPIs will identify more appropriate measurements to inform Leadership Group on progress.

Primary evidence in support of plan
Updated item 1 Records management maturity model
Updated item 8 Records management policy
Updated item 9 Records management strategy
Item 90 Leadership Group compliance report

Maturity model (I1) – Monitoring and reporting on records and information management
The SPCB will identify performance measures that reflect their information needs and put in place the means by which performance can be measured. Monitoring should be undertaken on a regular basis and the results reported to the person with lead responsibility for records management so that risks can be assessed and appropriate action taken.

Current level of maturity – 2 – Defined (updated)

Planned activity 13.2 Key performance indicators
Following implementation of the document retention policy, review and establish new KPIs concerning business as usual activities.
Element 14 – Shared information

The Scottish Parliament is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. The Scottish Parliament operates in accordance with the Information Commissioner’s Data sharing code of practice.

**Primary evidence in support of plan**

- Item 48 Data protection framework, including: Data protection policy, policy on managing the rights of data subjects, policy on data sharing and policy on management of data breaches
- Item 58 Data sharing guidance
- Item 59 Data sharing checklist

**Secondary evidence in support of plan**

- Updated item 1 Records management maturity model

---

**Maturity model (H1 & H2) – Records created in the course of collaborative working or through out-sourcing**

**H1** Records management controls should be applied to information being shared with or passed to other bodies or being held by another organisation on the SPCB's behalf.

**Current level of maturity** – 2 - Defined

**H2** When working in partnership with other organisations which includes sharing information and contributing to joint records systems, the SPCB will ensure that all participating staff are aware of the records management implications and that all parties agree protocols that specify: a) What information should be contributed and kept and by whom; b) What level of information security should be applied; c) Who should have access to the records; d) What disposal arrangements should be in place; and e) Which body holds the information for the purposes of the Act.

**Current level of maturity** – 1 - Aware

---

**Planned activity 14.1 Sharing records**

Measures will be put in place to define specific arrangements for information sharing and to actively control the management of the records the Scottish
Parliament owns, but does not hold. Measures will include ensuring consistent security access controls and application of retention and disposal actions.

**Planned activity 14.2 Management controls**

The Scottish Parliament will establish a set of management controls to be adopted by all staff when exchanging records with external bodies.
# Planned activity updates

<table>
<thead>
<tr>
<th>Planned activity 3.1</th>
<th>Complete – the records management policy and records management procedures were updated and signed off by Leadership Group on 27 January 2017. Updated evidence items 8, 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planned activity 4.1</td>
<td>Complete – the file plan has been successfully implemented in SPShare and is being used to fulfil business as usual requirements. Updated evidence item 17</td>
</tr>
<tr>
<td>Planned activity 4.2</td>
<td>Complete – file plan guidance has been implemented within the updated Records management procedures and guidance. Updated evidence items 12</td>
</tr>
<tr>
<td>Planned activity 5.1</td>
<td>Ongoing – the retention schedule will be reviewed and updated during the Document retention and good practice project to reflect updated requirements.</td>
</tr>
<tr>
<td>Planned activity 5.2</td>
<td>Complete – procedures document and guidance have been updated to reflect new processes following implementation of the DRM system. Updated evidence items 12 New evidence items 86, 87, 88 and 89</td>
</tr>
<tr>
<td>Planned activity 5.3</td>
<td>Complete – retention rules are applied to records automatically, determined by their location within the file plan. Rule automation documented in Records management procedures. Updated evidence item 12</td>
</tr>
<tr>
<td>Planned activity 5.4</td>
<td>Partially complete – the DRM system has been implemented across the SPS enabling monitoring of records retention and disposition from the Records Centre. An activity will be scoped to store and manage hardcopy vital records in a controlled and audited environment. Updated evidence item 12</td>
</tr>
<tr>
<td>Planned activity 6.1</td>
<td>Complete – destruction process and arrangements documented in Records management procedures. Updated evidence item 12</td>
</tr>
<tr>
<td>Planned activity 6.2</td>
<td>Ongoing – while the DRM system enables the deletion of records within the system, an activity to ensure all information is deleted and that this process is documented is required. This activity will be scoped and completed prior to the next RMP.</td>
</tr>
<tr>
<td>Planned activity 6.3</td>
<td>Ongoing – paper disposition within the DRM system to be investigated and a process for recording hardcopy destruction within the DRM system implemented.</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Planned activity 7.1</td>
<td>Ongoing – while the DRM system has been implemented, making it possible to export records to the NRS, arrangements will be made to explore the transfer process prior to the Scottish Parliament’s first transfer to the NRS on 01/01/2019.</td>
</tr>
<tr>
<td>Planned activity 7.2</td>
<td>Ongoing – following confirmation of the archiving process from SPShare, guidance will be updated.</td>
</tr>
<tr>
<td>Planned activity 8.1</td>
<td>Complete – protective marking has been refined and implemented across the Scottish Parliamentary Service. Updated evidence item 32</td>
</tr>
<tr>
<td>Planned activity 8.2</td>
<td>Complete – procedures and guidance documentation has been updated to reflect new processes following implementation of the DRM system. Updated evidence items 8, 12 New evidence items 86, 87, 88 and 89</td>
</tr>
<tr>
<td>Planned activity 9.1</td>
<td>Ongoing – DRM system has been implemented. An activity will be scoped to identify records managed outside the new system.</td>
</tr>
<tr>
<td>Planned activity 9.2</td>
<td>Complete – roles for overseeing and maintaining access restrictions have been assigned as business-as-usual. Evidence item 92</td>
</tr>
<tr>
<td>Planned activity 10.1</td>
<td>Ongoing – activity to be scoped and implemented</td>
</tr>
<tr>
<td>Planned activity 10.2</td>
<td>Ongoing - activity to be scoped and implemented</td>
</tr>
<tr>
<td>Planned activity 10.3</td>
<td>Ongoing - activity to be scoped and implemented</td>
</tr>
<tr>
<td>Planned activity 10.4</td>
<td>New – activity to document arrangements disaster recovery for the DRM environment.</td>
</tr>
<tr>
<td>Planned activity 11.1</td>
<td>Complete – DRM system has been fully implemented, enabling the complete auditing of records centre activities. Evidence item 72 Updated evidence item 91</td>
</tr>
<tr>
<td>Planned activity 11.2</td>
<td>Ongoing – external items to be scoped and implemented.</td>
</tr>
<tr>
<td>Planned activity 12.1</td>
<td>Ongoing – all staff have been trained to use the new DRM system. Business-as-usual training is under development. Updated evidence item 12</td>
</tr>
<tr>
<td>Planned activity 12.2</td>
<td>New evidence items 86, 87, 88 and 89</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>New</strong> – evidence (items 74 to 77) will be updated to reflect performance management changes.</td>
</tr>
<tr>
<td>Planned activity 13.1</td>
<td>Complete – maturity model reviewed following DRM project completion.</td>
</tr>
<tr>
<td></td>
<td>Updated evidence item 1</td>
</tr>
<tr>
<td>Planned activity 13.2</td>
<td>Partially complete – KPIs supporting the implementation of the document retention policy are presented to Leadership Group in the compliance report. Business-as-usual KPIs will be introduced post-document retention and good practice project.</td>
</tr>
<tr>
<td></td>
<td>New evidence item 88</td>
</tr>
<tr>
<td>Planned activity 14.1</td>
<td>Ongoing – activity to be scoped and implemented</td>
</tr>
<tr>
<td>Planned activity 14.2</td>
<td>Ongoing – activity to be scoped and implemented</td>
</tr>
</tbody>
</table>
## Annex A – Evidence

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01*</td>
<td>Records management maturity model</td>
<td>Jan 2017</td>
<td>All</td>
</tr>
<tr>
<td>06*</td>
<td>Statement of responsibility for records management</td>
<td>Jan 2017</td>
<td>1, 2, 12</td>
</tr>
<tr>
<td>11</td>
<td>Leadership Group sign off of records management policy</td>
<td>Feb 2012</td>
<td>3</td>
</tr>
<tr>
<td>12*</td>
<td>Records management procedures and guidance</td>
<td>Jan 2017</td>
<td>3, 5, 6, 7,</td>
</tr>
</tbody>
</table>
## Records management plan – 2016

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Metadata standard</td>
<td>Nov 2007</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>File plan workshops participant role</td>
<td>Jan 2013</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>File plan workshops presentation</td>
<td>Jan 2013</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>File plan workshops – summary of outcomes</td>
<td>Feb 2013</td>
<td>4</td>
</tr>
<tr>
<td>17*</td>
<td>File plan</td>
<td>Jan 2017</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>Records retention schedule</td>
<td>Apr 2012</td>
<td>5, 6, 7</td>
</tr>
<tr>
<td>19</td>
<td>Recycling and waste management services contract extract</td>
<td>Feb 2013</td>
<td>6</td>
</tr>
<tr>
<td>20</td>
<td>Recycling and waste management services – destruction certificate</td>
<td>Dec 2013</td>
<td>6</td>
</tr>
<tr>
<td>21</td>
<td>Recycling and waste management services – log book extract</td>
<td>Nov 2013</td>
<td>6</td>
</tr>
<tr>
<td>22</td>
<td>Records destruction form (small-scale)</td>
<td>May 2012</td>
<td>6</td>
</tr>
<tr>
<td>23</td>
<td>Records destruction guidance</td>
<td>May 2012</td>
<td>6</td>
</tr>
<tr>
<td>24</td>
<td>Off-site records and media tape storage contract</td>
<td>Jun 2010</td>
<td>6, 10</td>
</tr>
<tr>
<td>25</td>
<td>Off-site records storage destruction certificate</td>
<td>Nov 2012</td>
<td>6</td>
</tr>
<tr>
<td>26</td>
<td>Memorandum of understanding with the NRS</td>
<td>Jan 2014</td>
<td>7</td>
</tr>
<tr>
<td>27</td>
<td>NRS transfer form</td>
<td>May 2011</td>
<td>8</td>
</tr>
<tr>
<td>28</td>
<td>Information security policy</td>
<td>Sep 2013</td>
<td>8, 9</td>
</tr>
</tbody>
</table>
# Records management plan – 2016

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Information security guide</td>
<td>Sep 2013</td>
<td>8</td>
</tr>
<tr>
<td>30</td>
<td>Off-network data handling guide</td>
<td>Jan 2012</td>
<td>8</td>
</tr>
</tbody>
</table>
| 31   | Leadership Group (2012) paper 081 – Business IT guidance: Off-network data handling  
| 32   | **Protective marking system**  
| 33   | Leadership Group (2014), minutes, 27 January 2014                               | Jan 2014   | 8          |
| 34   | Security incident reporting procedure                                            | Feb 2014   | 8          |
| 35   | Security access arrangements for network shared drives                           | Feb 2014   | 8          |
| 36   | Process for creating network shares                                              | Jun 2009   | 8          |
| 37   | Email for checking permission to be granted                                      | May 2009   | 8          |
| 38   | Password protection and encryption                                               | Feb 2014   | 8          |
| 39   | Assyst knowledge base procedures                                                 | Accessed Feb 2014 | 8 |
| 40   | Encryption guidance                                                              | Accessed Feb 2014 | 8 |
| 41   | Protection of servers and electronic data                                        | Feb 2014   | 8          |
| 42   | Server build                                                                     | Jul 2011   | 8          |
## Records management plan – 2016

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>Description of electronic backups arrangements</td>
<td>Feb 2014</td>
<td>8</td>
</tr>
<tr>
<td>44</td>
<td>Security manuals</td>
<td>Feb 2014</td>
<td>8</td>
</tr>
<tr>
<td>45</td>
<td>Performance and capacity management report</td>
<td>Jan 2013</td>
<td>8</td>
</tr>
<tr>
<td>46</td>
<td>Account audit</td>
<td>Nov 2013</td>
<td>8</td>
</tr>
<tr>
<td>47</td>
<td>Routine information security reports</td>
<td>Feb 2014</td>
<td>8</td>
</tr>
<tr>
<td>48</td>
<td>Leadership Group (2014) paper 002, Data protection framework, including:</td>
<td>Feb 2014</td>
<td>8, 9, 14</td>
</tr>
<tr>
<td></td>
<td>• Data protection policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policy on managing the rights of data subjects</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policy on data sharing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policy on management of data breaches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Data protection guidance</td>
<td>Sep 2012</td>
<td>9</td>
</tr>
<tr>
<td>50</td>
<td>Subject access request guidance</td>
<td>Accessed</td>
<td>8, 9</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.parliament.scot/FoI/How_the_Parliament_responds_to_SARs.pdf">http://www.parliament.scot/FoI/How_the_Parliament_responds_to_SARs.pdf</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Guidance on processing subject access requests</td>
<td>Feb 2014</td>
<td>9</td>
</tr>
<tr>
<td>52</td>
<td>Subject access checklist</td>
<td>Feb 2014</td>
<td>9</td>
</tr>
<tr>
<td>53</td>
<td>Personal data breach plan and guidance</td>
<td>Feb 2014</td>
<td>9</td>
</tr>
<tr>
<td>54</td>
<td>Privacy impact assessment guidance</td>
<td>Sep 2010</td>
<td>9</td>
</tr>
<tr>
<td>55</td>
<td>Privacy impact assessment - project guidance</td>
<td>Jan 2013</td>
<td>9</td>
</tr>
<tr>
<td>56</td>
<td>Privacy impact assessment template</td>
<td>Jan 2013</td>
<td>9</td>
</tr>
<tr>
<td>57</td>
<td>Data protection training</td>
<td>Accessed</td>
<td>9</td>
</tr>
<tr>
<td>Item</td>
<td>Evidence detail</td>
<td>Date</td>
<td>Element(s)</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>58</td>
<td>Data sharing guidance</td>
<td>Feb 2014</td>
<td>9, 14</td>
</tr>
<tr>
<td>59</td>
<td>Data sharing checklist</td>
<td>Feb 2014</td>
<td>9, 14</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.parliament.scot/SPCB/1207_paper_60.pdf">http://www.parliament.scot/SPCB/1207_paper_60.pdf</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>SPCB minutes</td>
<td>Dec 2011</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.parliament.scot/SPCB/SPCB-11-14-M_07-12-11_minutes.pdf">http://www.parliament.scot/SPCB/SPCB-11-14-M_07-12-11_minutes.pdf</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Leadership Group (2013) paper 063 – further development of BC plans</td>
<td>Nov 2013</td>
<td>10</td>
</tr>
<tr>
<td>64</td>
<td>Blank template – Office business continuity plan</td>
<td>Accessed</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Feb 2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>AAB paper</td>
<td>Sep 2013</td>
<td>10</td>
</tr>
<tr>
<td>66</td>
<td>BCAP paper 07/4 Sep 2012 – salvage plan development</td>
<td>Sep 2013</td>
<td>10</td>
</tr>
<tr>
<td>67</td>
<td>BCAP minutes, 20 September 2012</td>
<td>Sep 2013</td>
<td>10</td>
</tr>
<tr>
<td>68</td>
<td>Leadership Group (2013) paper 06 (extract)</td>
<td>Jan 2013</td>
<td>10</td>
</tr>
<tr>
<td>69</td>
<td>Vital records recommendations</td>
<td>Jan 2013</td>
<td>10</td>
</tr>
<tr>
<td>70</td>
<td>Hardcopy records storage inventory</td>
<td>Feb 2014</td>
<td>11</td>
</tr>
<tr>
<td>71</td>
<td>Hardcopy records storage retrieval tracking</td>
<td>Feb 2014</td>
<td>11</td>
</tr>
</tbody>
</table>
## Records management plan – 2016

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>72</td>
<td>DRM system audit log settings</td>
<td>Aug 2013</td>
<td>11</td>
</tr>
<tr>
<td>73</td>
<td>Records manager job vacancy</td>
<td>2007</td>
<td>2, 12</td>
</tr>
<tr>
<td>74</td>
<td>Performance management template – Information Manager Standard template</td>
<td>2013</td>
<td>12</td>
</tr>
<tr>
<td>75</td>
<td>Performance management system</td>
<td>Accessed Feb 2014</td>
<td>12</td>
</tr>
<tr>
<td>76</td>
<td>Professional development plan</td>
<td>November 2013</td>
<td>12</td>
</tr>
<tr>
<td>77</td>
<td>Professional development plan guidance</td>
<td>Accessed Feb 2014</td>
<td>12</td>
</tr>
<tr>
<td>78</td>
<td>Records management champion training plan</td>
<td>Mar 2009</td>
<td>12</td>
</tr>
<tr>
<td>79</td>
<td>Records management champion training programme</td>
<td>Mar 2009</td>
<td>12</td>
</tr>
<tr>
<td>80</td>
<td>Recycling and disposal of IT equipment contract extract</td>
<td>March 2013</td>
<td>6</td>
</tr>
<tr>
<td>81</td>
<td>Recycling and disposal of IT equipment - Disposal list template</td>
<td>Accessed May 2014</td>
<td>6</td>
</tr>
<tr>
<td>82</td>
<td>Recycling and disposal of IT equipment - Disposal collection template</td>
<td>Accessed May 2014</td>
<td>6</td>
</tr>
<tr>
<td>83</td>
<td>Recycling and disposal of IT equipment - Disposal confirmation extract</td>
<td>August 2013</td>
<td>6</td>
</tr>
<tr>
<td>84</td>
<td>RM intranet homepage</td>
<td>Accessed May 2014</td>
<td>3</td>
</tr>
</tbody>
</table>
# Records management plan – 2016

<table>
<thead>
<tr>
<th>Item</th>
<th>Evidence detail</th>
<th>Date</th>
<th>Element(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>86**</td>
<td>SPShare training material – InfoPods</td>
<td>2015</td>
<td>3</td>
</tr>
<tr>
<td>87**</td>
<td>SPShare training material – quick reference guides</td>
<td>2015</td>
<td>3</td>
</tr>
<tr>
<td>88**</td>
<td>SPShare training material – session slides</td>
<td>2015</td>
<td>13</td>
</tr>
<tr>
<td>89**</td>
<td>SPShare training material – session plan</td>
<td>2015</td>
<td></td>
</tr>
<tr>
<td>90**</td>
<td>Leadership Group (2106) paper 057 – Q2 compliance report</td>
<td>Oct 2016</td>
<td>13</td>
</tr>
<tr>
<td>91**</td>
<td>Document and records management project closure report</td>
<td>Mar 2017</td>
<td>11</td>
</tr>
<tr>
<td>92**</td>
<td>SPShare security group changes process</td>
<td>Apr 2017</td>
<td>9</td>
</tr>
</tbody>
</table>

* updated evidence item

** new evidence item

All URL links last accessed June 2017