The Scottish Parliament
Pàrlamaid na h-Alba

The Scottish Parliament
The Scottish Parliamentary Corporate Body
The Scottish Commission for Public Audit

Records management plan – 2023

Plana rianachd chlàran – 2023

This 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.

The plan, prepared by the Scottish Parliamentary Service (SPS), sets out proper arrangements for the management of public records created, managed and disposed of by the Scottish Parliament, the Scottish Parliamentary Corporate Body 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 Parliamentary Service (SPS) recognises that records management is vital for the proper functioning of any organisation and is essential in ensuring that the Parliament has accurate, reliable and accessible records of its work to support its business and maintain a sufficient archive of its activities.

This Records management plan sets out what has been done to improve the records management function in the SPS 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 Parliamentary Service (SPS) in this plan include the Scottish Parliament, the Scottish Parliamentary Corporate Body and the Scottish Commission for Public Audit. The Scottish Parliamentary Service is the collective term for the group of professional staff employed by the Scottish Parliamentary Corporate Body to support the business and operations of the Scottish Parliament and the Scottish Commission for Public Audit.

Plan structure

For each element, the plan reviews the SPS'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 SPS plans to improve records management maturity.

The records management maturity model (evidence item 1) 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

3 Embedded – the effective management of records is fully integrated within strategic and operational activities

Background

Records management is a strategic priority for the SPS and a key activity in establishing the SPS as an exemplar of good governance, excellent resource management and accountability.

SPS digital records have been managed in SharePoint Online since 2021.

Paper records are managed at box level and stored in either an internal storage facility, managed by information management staff or with a records storage contractor in an off-site storage facility.

Recent activities

Digital Workplace Programme (2020 - 2023)

The Digital Workplace Programme co-ordinated a series of project-level initiatives with a common goal of migrating the SPS's information from internal server-based technologies to the Microsoft 365 platform, replacing ageing technologies, and providing users with access to modern, digital solutions that support new ways of working. SharePoint (SP) Online replaced SharePoint 2013 (SPShare) as the primary document and records management (DRM) system of the SPS.

The vision for the Digital Workplace Programme supported the SPS's Digital Strategy to demonstrate a "smart, confident use of technology and information to drive improvements in how we collaborate, communicate and deliver the business of the Parliament."

The main business drivers for the programme were to:

- Reduce the future operating costs
- Support continuous improvement
- Provide staff with modern tools that will enable them to work more productively

Key initiatives:

The vision for the new cloud-based document and records management system was to:

- simplify the existing DRM architecture
- remove the duplication of services e.g., between the Intranet and SharePoint 2013, and reduce handling errors
- provide more efficient DRM (reducing the input required from staff and refining records management processes to reduce administrative overhead for Information management staff)
- improve business continuity and access to information

Digital records management system

The SPS has implemented Microsoft 365 with E3 licenses to enable online collaboration and effective management of digital public records. AvePoint's Cloud Records application has been implemented to address the recordkeeping requirements to be met over and above functionality provided within M365 native E3 functionality.

Classification

AvePoint Cloud Records uses and synchronises the existing SPS Business classification scheme (BCS) within the SPS M365 environment. BCS terms applied to records within SP Online are synchronised with AvePoint Cloud Records enabling the management of record lifecycles within the AvePoint Cloud Records interface.

BCS terms applied to documents are used to capture, and make immutable, records and apply retention and disposal rules. All records environments are visible in one interface making it possible to associate BCS terms with rules for retention or disposal, apply term settings, and assign content to business functions regardless of location.

Retention and disposition

The records lifecycle is managed through the AvePoint Cloud Records interface for content which enables:

- the association of lifecycle outcomes with business rules that remove, retain, destroy or archive records
- the addition of records metadata to content as part of a business rule
- the application of business rules to trigger lifecycle outcomes based on actions or metadata.
- the automation of rules in addition to manual approvals

Auditing and reporting

AvePoint Cloud Records maintains and enables reporting on all actions performed on items or by a user to ensure system governance. The Records Manager can view reports on the Records Management Dashboard, including managed records, destroyed records, records that have outstanding approval actions, etc.

Element 1 – Senior management responsibility

An individual senior staff member is identified as holding corporate responsibility for records management.

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

Alan Balharrie
Chief Information Officer and Group Head for Digital Services
The Scottish Parliamentary Corporate Body
The Scottish Parliament
Edinburgh
EH99 1SP

A statement of responsibility (evidence item 2) is supplied with the records management plan to confirm that Alan Balharrie endorses the SPS's records management policy (evidence item 3).

Records management has the full support of the SPS's senior managers. The Strategic plan (evidence item 4), and the associated corporate values, demonstrates the SPS's commitment to ensuring accountability, improvement and using our skills and resources to deliver high-quality results are core to all activities carried out by the SPS.

Primary evidence in support of plan

Evidence item 2 Statement of responsibility for records management – Alan Balharrie

Secondary evidence in support of plan

Evidence item 3 Records management policy

Evidence item 4 Strategic plan

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

An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.

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

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

The Information Manager has overall day-to-day responsibility for records management and the implementation of the SPS's Records management plan. Evidence item 5 confirms that the Information Manager is the person responsible for implementing the Records management plan. Roles and responsibilities are further defined in the SPS's Records management policy (evidence item 3).

The Information Manager's office, Information Management and Governance, is an office within the Digital Services Group which also includes Business Information Technology. The Information Manager works closely with IT colleagues and is a key stakeholder in M365 developments in the SPS. As Product Owner of Documents and Records Management in M365 in the Digital Workplace Programme the Information Manager led the development and implementation of records management solutions in M365. The Information Manager has developed expertise on managing records in M365 with AvePoint Cloud Records and is accountable for the development and ongoing management of records management solutions in M365.

The Information Manager has been assigned *Global Reader* access to the M365 admin center giving access to the Microsoft Purview compliance portal which enables the Information Manager to manage day-to-day records management which includes access to reports which assist in managing M365 information and records (evidence item 56). In addition, as an administrator of AvePoint Cloud Records the Information Manager and Information management staff have complete access to all records activities within the tool (evidence item 57).

Primary evidence in support of plan

Evidence item 5 Statement of responsibility for records management – Gordon Hobbs

Evidence item 56 M365 Manage admin roles

Evidence item 57 AvePoint Online Services service administrators

Secondary evidence in support of plan

Item 3 Records management policy

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

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.

Current level of maturity – 3 - Embedded

Element 3 – Records management policy statement

The authority has an appropriate policy statement on records management.

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

The SPS Records management strategy (evidence item 6) and Policy (evidence item 3) were endorsed by Alan Balharrie, Chief Information Officer and Group Head for Digital Services in June 2021 (evidence item 2).

In support of the Strategy and Policy, Records management procedures (evidence item 7) have 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 SPS creates, receives and shares. Records management procedures were updated following implementation of SP Online and training material (evidence items 54-56) developed to provide guidance on SP Online features. SP Online is the central repository for SPS records and records created in other systems, such as email, are required to be transferred to SP Online to ensure their management.

The strategy, policy and procedures documents are published on the records management SP Online site, available to all SPS staff (evidence items 8), in addition to other reference material. SP Online training material complements the Records management procedures and is available to all staff on the SP Online help site, on the dedicated https://scottish4.sharepoint.com/sites/corp-help-spol (evidence item 9).

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 (evidence item 10). The metadata of disposed records is maintained permanently in the system, in the repository where the original record was located.

Primary evidence in support of plan

Evidence item 2 Statement of responsibility for records management – Alan Balharrie

Evidence item 3 Records management policy

Evidence item 6 Records management strategy

Evidence item 7 Records management procedures

Evidence item 9 SP Online help site

Evidence item 10 Controlled DRM metadata

Secondary evidence in support of plan

Evidence item 1 Records management maturity model

Evidence item 7 Records management procedures

Evidence item 8 Records management SP Online site home page

Evidence item 9 SP Online help site home page

Evidence item 10 Controlled DRM metadata

Evidence item 56 Records management awareness course

Maturity model (B) – Records management policy

B1 The SPCB will issue a policy covering records management. This should be endorsed by the Chief Information Officer and be readily available.

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 scheme

Records are known and are identified within a structure, ideally founded on function.

The SPS Business classification scheme (BCS) in M365 is a Term Set within the M365 Term Store Management Tool. The Term Set is made available to SP Online documents through the *Record classification* column which is a Managed Metadata column published to all Content Types used in SP Online.

Changes to the BCS are made within AvePoint Cloud Records which in turn publishes changes to the Term Store Management Tool and SP Online. AvePoint Cloud Records uses the terms in the BCS to apply to documents in SP Online enabling the management of records capture, retention, and disposition.

The BCS is structured by a class-item hierarchy 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 (evidence item 11).

Within SP Online (including document libraries connected to Teams) the BCS is available as metadata to all documents and records through the *Record classification* column which is available on all content types. SP Online automatically assigns a Record classification according to the location a document. The SPS operates in-place records management in SP Online and each document library (and often folders within libraries) are assigned a default BCS term in AvePoint Cloud Records which ensures that all content in that location receives a BCS term at the point of creation.

A document's location determines if it will be automatically assigned the *Unclassified* term, which will result in it being managed as a document and subsequently deletion 24 months from last modification or assigned another BCS term which results in it being managed as record. Documents with a *Record classification* other than *Unclassified* are automatically captured as records following 100 days of inactivity using an AvePoint Cloud Records rule. From this point documents are immutable and managed by the rules defined in AvePoint Cloud Records. AvePoint Cloud Records rules mirror record series retention requirements in the records retention schedule.

The BCS reflects the functions and activities undertaken by the SPS and is updated regularly by Information management staff to reflect any changes. New terms are added regularly to ensure that records are managed appropriately. For example, new projects, contracts, Bills and Committee inquiries etc. are added frequently.

When new SP Online sites are created for a new project, contract etc. a new BCS term is created and associated with the site in AvePoint Cloud Records (evidence item 58) to ensure records are captured.

Where new records are created in specific folders (Document sets), for example a new Bill or Committee inquiry, Microsoft Flows are in place (evidence item 59) to alert Information management staff to the requirement for a new BCS term. Following

notification, Information management staff add a new term to the BCS and assign the term to the Document set to ensure records are captured (evidence item 60).

Primary evidence in support of plan

Evidence item 11 Business Classification Scheme

Evidence item 58 New BCS term - site

Evidence item 59 New BCS term - inquiry alert

Evidence item 60 New BCS term - Document set

Secondary evidence in support of plan

Evidence 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

Element 5 – Retention schedule

Records are retained and disposed of in accordance with the Retention Schedule

The records retention schedule (evidence item 12) was last reviewed and signed off in January 2021. It was signed off by each Office Head and the Office for the Solicitor of the Scottish Parliament and was made available to NRS for comment to ensure that SPS obligations to preserve records with NRS were reflected appropriately.

In addition to the records retention schedule, the SPS has records management procedures (evidence item 7), offering practical guidance to staff on the creation, use, management and disposal of records. The procedures describe how the SPS 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 BCS automatically which then enables the application of retention rules based on pre-defined criteria e.g., location. Retention rules are associated with individual terms in the BCS which means that all individual records classified with terms are managed consistently regardless of location within SP Online. Event-based retention is possible using AvePoint Cloud Records to ensure that records concerning the same activity are retained for the same period as defined in the retention schedule. The AvePoint Cloud Records system prompts information management staff on the need to review records using pre-defined metadata.

A document and communications retention policy (evidence item 13) is also in place which requires that documents and email, not captured as records, are automatically deleted if they have not been modified for 24 months, instant messaging (Teams chat) for 7 days and discussion forum conversations (Teams channels) for 1 year. This policy helps ensure that SPS staff have a defined and consistent approach to managing the retention of documents and communications not subject to the records retention schedule.

Primary evidence in support of plan

Evidence item 7 Records management procedures

Evidence item 12 Records retention schedule

Evidence item 13 Communications and document retention policy

Secondary evidence in support of plan

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

Planned activity 2023-05-01

Centralisation of records. Identify and investigate steps to automate application of records retention schedule to records held in systems outwith M365.

Element 6 – Destruction arrangements

Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.

Hardcopy records

The SPS 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 14). The contractor provides a confidential destruction and recycling service in compliance with EN15713:2009. A certificate of destruction (evidence item 15) is provided for each destruction actioned by the contractor. In addition, an internal logbook (evidence item 16) 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 17) available to all staff and contractors on the intranet and additionally record destruction activity on a form. Guidance is available for staff to follow (evidence item 18).

Hardcopy non-current records that need to be kept for a pre-determined period are sent to an off-site storage contractor (evidence item 19). Records destroyed by the off-site storage contractor are shredded, pulped and recycled with a destruction certificate (evidence item 20) 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 21).

Digital records

Digital documents in SP Online that do not meet the criteria of a record are automatically assigned the *Unclassified* Records classification. *Unclassified* documents are automatically deleted following 24 months of inactivity in accordance with the Documents and communications retention policy. Furthermore, it is the policy of the SPS that information that would normally be considered a record should be managed in SP Online. Other short-term information held in other M365 tools for example Microsoft Teams should not be relied on for storing records – Teams chats are automatically deleted after 7 days (evidence item 13).

Policy requires that digital records are captured and managed by SPS staff in SP Online where they are automatically assigned a BCS term (determined by location) which in turn ensures their proper management and destruction in a controlled, secure and irretrievable way using the AvePoint Cloud Records application.

Records reaching the end of their assigned retention period are listed in the “Records for review” section of AvePoint Cloud Records and assigned to a member of the Information management team for review and action. Individual items are listed in the “Records for review section” but it is possible to destroy records in bulk by making use of the BCS to destroy records associated one BCS term, a records class or other captured metadata.

Destruction is actioned following a 3-stage process where the Information Officer seeks authorisation from the relevant business area before approving destruction themselves. The Information Manager has final authority to approve destruction at which point records are deleted. Disposition stubs with original metadata replace deleted records in SP Online sites and destruction logs are retained in AvePoint Cloud Records as evidence of destruction actions (evidence item 22). Destruction audit logs can be exported from AvePoint Cloud Records for permanent retention elsewhere. Email chains between information management staff and business areas are captured as records in addition to the AvePoint Cloud Records audit log.

As an added precaution, all end of use data-bearing IT equipment is securely sanitised or destroyed to “Secure Sanitisation Level (SSL) 2 Clear” as defined in His Majesty’s Government Information Assurance 5 - Secure Sanitisation of Protectively Marked Information or Sensitive Information (HMG IA 5). For certain items deemed to contain more highly sensitive data, disposition conforms to “SSL2 Purge” or “Destroy” sanitisation in accordance with CPNI Standard (April 2014) Secure Destruction of Sensitive Items © Crown copyright 2014 (evidence item 23).

Primary evidence in support of plan

Evidence item 13 Document and communications retention policy

Evidence item 14 Recycling and waste management services contract extract

Evidence item 15 Recycling and waste management services destruction certificate

Evidence item 16 Recycling and waste management services log-book extract

Evidence item 17 Records destruction form (small-scale)

Evidence item 18 Records destruction guidance

Evidence item 19 Off-site records storage contract extract

Evidence item 20 Off-site records storage destruction certificate

Evidence item 21 Offsite storage service web-based inventory tool

Evidence item 22 DRM system disposal metadata

Evidence item 23 Recycling and disposal of IT equipment contract extract

Secondary evidence in support of plan

Evidence item 1 Records management maturity model

Evidence item 7 Records management procedures

Evidence item 12 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

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

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

Planned activity 2023-06-01

A paper disposition recording process using AvePoint Cloud Records will be investigated.

Element 7 – Archiving and transfer arrangements

Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'.

The SPS has in place arrangements to dispose records of archival value with National Records of Scotland (NRS). NRS and the SPS are guided by a Memorandum of Understanding (evidence item 24) and NRS is given the opportunity to provide feedback on the SPS records retention schedule which identifies the records selected for permanent preservation. The Records management procedures (evidence item 7) details the process for transferring records identified by the retention schedule for permanent preservation with NRS.

AvePoint Cloud Records retention rules enables records identified for historical preservation to be identified as such by the application of an associated rule. Record classification can be used to export all records associated with a classification regardless of location within SP Online. Exported records are exported along with original metadata.

In order to facilitate export and/or transfer of records from the DRM system, AvePoint Cloud Records has a choice of 3 records export features (evidence item 26) – VERS Encapsulated Objects (VEO), National Archives of Australia (NAA) or National Archives and Records Administration (NARA) export formats (evidence item 26).

Primary evidence in support of plan

Evidence item 24 Memorandum of understanding between the Scottish Parliament and the NRS

Evidence item 25 NRS transfer form

Evidence item 26 NARA config file

Secondary evidence in support of plan

Evidence item 7 Records management procedures

Evidence item 12 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 – 2 - Defined

Planned activity 2023-07-01

Review and update the Memorandum of understanding with NRS

Planned activity 2023-07-02

Review options for exporting records to NRS with AvePoint and explore possibility of making available NRS-approved export format for Cloud Records

Planned activity 202307-03

Transfer of Session 1 (1999-2003) digital records to NRS

Element 8 – Information security

Records are held in accordance with information security compliance requirements.

The SPS has well-established policies and procedures concerning the security of its information. The information security policy (evidence item 27) covers information, data, software, hardware, and communication networks for which the Business Information Technology (BIT) office is the custodian.

The SPS protective marking system (evidence item 28) provides a layer of security for information contained within documents (including email) 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 SPS's information assets:

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

M365 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 (Data Loss Prevention).

The SPS has an agreed password policy for users of its systems (not submitted as evidence for IT security reasons but demonstrable upon request). Our knowledge base holds password guidance on identity management, securing parliament data on mobile devices with passwords, administrative passwords being held under strong encryption and with appropriate role-based access control in place. Networking equipment is secured by password and access is monitored and logged.

Remote users must go through multi-factor authentication (biometric app-based or SMS second factors) and/or certificate-based authentication. This can be demonstrated if required.

All laptops and remote office PCs with the SPS build are encrypted by BITlocker encryption as part of the SPS standard desktop build, which can be demonstrated upon request. The SPS also has encryption guidance on how BITlocker can be used to secure removable media. Mobile devices used to access Parliament data must be encrypted.

Primary evidence in support of plan

Evidence item 27 Information security policy

Evidence item 28 Protective marking system

Evidence item 29 Sharing agreement

Evidence item 30 Removal risk assessment

Evidence item 31 Managing information remotely

Evidence item 32 Security incident reporting form

Secondary evidence in support of plan

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

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

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

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.

Current level of maturity – 3 – Embedded

Planned activity 2023-08-01

Review and analysis of data loss prevention tools in M365

Planned activity 2023-08-02

Implementation of measures to prevent M365 access from personal devices without mobile device management software

Element 9 – Data protection

Records involving personal data are managed in compliance with data protection law.

The SPS has a legal obligation to comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, ensuring that it has arrangements in place to manage, process and protect personal data. The SPS's data protection policy (evidence item 33) 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 and is also the Data Protection Officer for the SPS. The Head of Information Governance takes the lead in ensuring the SPS is fulfilling its legislative obligations.

The guide to submitting subject access requests to the SPS is available on the Scottish Parliament website (evidence item 34). The Scottish Parliamentary Corporate Body is registered with the Information Commissioner as required by the Data Protection Act 2018, registration number Z7477607.

The Information Management and Governance team has responsibility for overseeing access restrictions to documents and records within M365, ensuring compliance with the Protective marking system. The management of individual security groups required for the proper functioning of protective marking and M365 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

Evidence item 33 Data protection policy

Evidence item 34 Subject access request guidance

Secondary evidence in support of plan

Evidence item 27 Information security policy

Evidence item 28 Protective marking system

Evidence item 35 Data protection impact assessment policy

Evidence item 36 Data breach policy

Evidence item 37 Data protection impact assessment questionnaire

Evidence item 38 Data protection processing conditions guide

Evidence item 39 Data sharing checklist

Evidence item 40 Privacy notice guidance and template

Evidence item 41 Privacy notices

Evidence item 42 Data protection roles and responsibilities

Evidence item 43 Data protection training

Evidence item 44 GDPR for SPCB Staff video

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

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

Element 10 – Business continuity and vital records

Record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.

The SPS 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 resilience strategy (evidence item 45). 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.

Business continuity and salvage plans show that the information resources required by offices to maintain business are almost wholly electronic.

M365, and more specifically, SP Online is the SPS's default document and records management system. M365 operates using distributed databases over several data centres. Microsoft's standard recoverability offering of 93 days is not sufficient for SPS business needs. The SPS therefore uses a third-party backup solution to back up documents and records held in M365 – Cloud Backup, a backup solution provided by AvePoint.

AvePoint Cloud Backup maintains a backup of data held in SP Online, Teams (documents) and OneDrive for Business for a period of 2 years – a backup is carried out daily. All data in backed up locations within M365 is backed up without exception. Data managed by Cloud Backup is stored in UK Azure Storage and data is backed up using immutable time-based policy containers. All communications are performed over HTTPS using TLS 1.2 and all data at rest is encrypted using AES 256.

Primary evidence in support of plan

Evidence item 45 Business continuity resilience strategy

Evidence item 46 Business continuity manual

Evidence item 47 Business continuity annual report

Secondary evidence in support of plan

Evidence item 19 Off-site records storage contract extract

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 – 2 - Defined

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 – 3 – Embedded

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

Planned activity 2023-10-01

Activity to review the concept of vital records, determine if such records need to be managed more rigorously than other records and to develop any required processes to manage records considered “vital”.

Element 11 – Audit trail

The location of records is known and changes recorded.

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 SPS 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 48). There are electronic and paper trails for all transactions relating to receipt, transfer, return and disposal of records held in storage (evidence item 49).

Digital records

The version history of all documents and records in SP Online is captured enabling the location and identification of changes. SP Online is configured to capture a maximum of 500 major versions of changes (evidence item 50).

In addition to version history, changes to documents in document repositories are captured by Microsoft 365 Unified Audit Logging. Unified auditing provides access to event logs (view, create, edit, upload, download, and delete) and sharing actions like invitation and access requests, and synchronisation activity (evidence item 51). Logs are retained for the M365 default period of 90 days.

AvePoint Cloud Records also maintains logs of activities. The Administrator Audit Report is used to display detailed information of activities, including operation records and export records performed within AvePoint Cloud Records within a specified time frame (evidence item 61). The Action Audit Report is used to display the user activities in the reporting scope by a specific time (evidence item 62). Cloud Records audit reports are retained for an indefinite period enabling long-term retention beyond M365 limitations.

Primary evidence in support of plan

Evidence item 7 Records management procedures

Evidence item 48 Hardcopy records storage inventory extract

Evidence item 49 Hardcopy records storage retrieval tracking

Evidence item 50 Version history

Evidence item 51 Audit log extract

Evidence item 61 Cloud Records Administrator Audit Report

Evidence item 62 Cloud Records Action Audit Report

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

Planned activity 2023-11-01

Investigation and implementation of measures to ensure local retention of unified audit log information related to records for as long as the record to which it relates

Element 12 – Records management training for staff

Staff creating, or otherwise processing records, are appropriately trained and supported.

The SPS Information Manager is responsible for records management in the SPS and is supported in the role by the senior responsible officer (evidence item 2). Adequate budget is in place for training and ongoing professional development to help ensure the Information Manager fulfils the role of Records Manager by:

- providing good practice through policies, procedures, and guidance
- ensuring all teams and individuals understand and can carry out their responsibilities
- ensuring records are fit-for-purpose
- ensuring records are created, retained, and disposed of in accordance with the SPCB records retention schedule (evidence item 3)

All staff are expected to complete an induction programme (evidence item 52) following recruitment and to continue to maintain appropriate knowledge and skills throughout their career in the SPS. Records management procedures (evidence item 7) are available to all staff on SP Online (evidence item 8).

All staff are expected to maintain appropriate skills by completing the Records management awareness course (evidence item 55) and referring to available guidance material when required (evidence items 53 and 54), to enable them to perform their duties and meet records management requirements.

Primary evidence in support of plan

Evidence item 2 Statement of responsibility for records management – Alan Balharrie

Evidence item 3 Records management policy

Evidence item 7 Records management procedures

Evidence item 8 Records management intranet page

Evidence item 52 Records management quick reference guide - induction

Evidence item 53 DRM system quick reference guides

Evidence item 54 DRM system InfoPods

Evidence item 55 Records management awareness course

Secondary evidence in support of plan

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 development.

Current level of maturity – 3 - Embedded

Planned activity 2023-12-01

Performance management. The Scottish Parliament's performance management system has been redeveloped and is currently being implemented. Element 12 and supporting evidence will be updated to reflect performance management changes.

Element 13 – Assessment and review

Records Management arrangements are regularly and systematically reviewed with actions taken when required.

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

Primary evidence in support of plan

Evidence item 1 Records management maturity model

Evidence item 3 Records management policy

Evidence item 6 Records management strategy

Secondary evidence in support of plan

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

Planned activity 2023-13-01

Key performance indicators. Review and establish KPIs concerning business as usual activities.

Element 14 – Shared information

Information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.

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

Evidence item 28 Protective marking system

Evidence item 29 Sharing agreement

Evidence item 30 Removal risk assessment

Evidence item 39 Data sharing checklist

Secondary evidence in support of plan

Evidence item 7 Records management procedures

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 – 3 - Embedded

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 – 2 - Defined

Element 15 – Public records created by third parties

Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.

None of the SPS's functions are managed by third parties and therefore no records are created by third parties.

Annex A – Evidence

Evidence item 1 Maturity model

Evidence item 2 Statement of responsibility for records management – Alan Balharrie

Evidence item 3 Records management policy

Evidence item 4 Strategic plan (Our Strategic Plan | Scottish Parliament Website)

Evidence item 5 Statement of responsibility for records management – Gordon Hobbs

Evidence item 6 RM strategy

Evidence item 7 Records management procedures

Evidence item 8 Records management site

Evidence item 9 SP Online help site

Evidence item 10 Controlled DRM metadata

Evidence item 11 BCS

Evidence item 12 Records retention schedule

Evidence item 13 Document and communications retention policy

Evidence item 14 Recycling and waste management services contract extract

Evidence item 15 Recycling and waste management services destruction certificate

Evidence item 16 Recycling and waste management services log-book extract

Evidence item 17 Records destruction form (small-scale)

Evidence item 18 Records destruction guidance

Evidence item 19 Off-site records storage contract extract

Evidence item 20 Off-site records storage destruction certificate

Evidence item 21 Offsite web based inventory tool

Evidence item 22 DRM system disposal metadata

Evidence item 23 Recycling and disposal of IT equipment contract extract

Evidence item 24 Memorandum of understanding between the Scottish Parliament and the NRS

Evidence item 25 NRS transfer form

Evidence item 26 NARA config file

Evidence item 27 Information security policy

Evidence item 28 Protective marking system

Evidence item 29 Sharing agreement

Evidence item 30 Removal risk assessment

Evidence item 31 Managing information remotely

Evidence item 32 Security incident reporting form

Evidence item 33 Data protection policy

Evidence item 34 Subject access request guidance

Evidence item 35 Data protection impact assessment policy

Evidence item 36 Data breach policy

Evidence item 37 Data protection impact assessment questionnaire

Evidence item 38 Data protection processing conditions guide

Evidence item 39 Data sharing checklist

Evidence item 40 Privacy notice guidance and template

Evidence item 41 Privacy notices (Privacy notices | Scottish Parliament Website)

Evidence item 42 Data protection roles and responsibilities

Evidence item 43 Data protection training

Evidence item 44 GDPR for SPCB Staff video (GDPR for SPCB Staff - YouTube)

Evidence item 45 Business continuity resilience strategy

Evidence item 46 Business continuity manual

Evidence item 47 Business continuity annual report

Evidence item 48 Hardcopy records storage inventory

Evidence item 49 Hardcopy records storage retrieval tracking

Evidence item 50 Version history

Evidence item 51 Audit log extract

Evidence item 52 Records management quick reference guide - induction

Evidence item 53 DRM system quick reference guides

Evidence item 54 DRM system InfoPods

Evidence item 55 Records management awareness course

Evidence item 56 M365 Manage admin roles

Evidence item 57 AvePoint Online Services service administrators

Evidence item 58 New BCS term - site

Evidence item 59 New BCS term - inquiry alert

Evidence item 60 New BCS term - Document set

Evidence item 61 Cloud Records Administrator Audit Report

Evidence item 62 Cloud Records Action Audit Report