Records Management Policy | 2024

Descriptor	Changes made	Date	Version	Approved By
Policy first implemented	Initially drafted and adopted in June 2020 (V0.2). Full revision completed during 2021. Formally reviewed and approved in May 2022.	7 May 2022	1.0	SLT
Review no.1	Full revision completed during 2021. Formally reviewed and approved in May 2024. Minor changes: Related Policies Removal of 2 policies at as now no longer relevant Addition of Business Classification Scheme Related SOPs Change of Business Continuity Plan to SOSE Business Continuity Management Policy Related Guidance Addition of Information Asset Register and SOSE Document Naming Convention Approved by Addition of SLT for Major Changes and Director of F&CR for Minor Changes Additional Points of Contact Amended DPO role title and added Records Management Executive 4.0 Definitions Added Information Asset Owner, Information Asset Custodian, and Senior Information Risk Oficer roles and descriptions.	6 June 2024	2.0	Director

Review no.2	Amendments due to Organisational Change	5 September 2025	2.0	Director of Business Enablement
Review no.3				
Review no.4				
Review no.5				

Name of policy being superseded (if applicable)	Records Management Policy	2022
Related policies	Data Protection Policy; Business Classification Scheme; Business Continuity Management Policy
Related SOPs	Using IT Equipment & Systems; SOSE Business Continuity Management Policy
Related Guidance	SOSE_Document_Naming_Convention; DRAFT_Document_Retention_Schedule; Information Asset Register
Equality Impact Assessment completed	No need to complete an EqIA for this policy, as any system accessibility issues related to disabled groups will be covered by other projects' impact assessments, e.g. Office 365
Intended Audience	All SOSE Staff
Team responsible for policy	Governance and Assurance Team
Policy owner contact details (email)	Director of Business Enablement (Allan.Harrow@sose.scot)
Approved by	SLT for Major Changes Director of Business Enablement for Minor Updates
Additional points of contact	Head of Governance and Assurance, Data Protection Officer Assurance and Resilience Business Partner
Policy due for review (date)	1 May 2026

Contents|

1.0   Policy Summary |

1.1   South of Scotland Enterprise (SOSE) information and records are a vital asset, enabling us to deliver and provide evidence of the work that we do and the decisions we make, supporting businesses and communities in the South of Scotland. This Policy ensures that we create, capture, and manage information efficiently and effectively to ensure that we have:

- The right information when we need it to make the right decisions
- The evidence we need to account for our actions and decisions allowing us to be open, transparent, and accountable, as well as, providing evidence of compliance
- The records required to uphold the rights and protect the interests of our organisation, our employees, external partners and the people and businesses in communities across the South of Scotland

2.0 Policy Purpose and Objectives |

2.1   This Policy statement sets out SOSE's expectations for colleagues to ensure the creation and capture of adequate records of all business activities and to managing them appropriately throughout their lifecycle in such a way that they:

- Meet our operational, financial, and strategic needs and our legal obligations
- Can be trusted to be accurate, up to date and reliable
- Are quickly and easily located, retrieved, identified and usable
- Are protected and stored securely
- Are accessible for as long as required and disposed of appropriately

2.2   The implementation of this policy will result in a number of benefits to the organisation, including:

- Increased accountability and transparency
- Informed decision making based on accurate, complete, and current information
- Compliance with statutory, regulatory, and contractual requirements
- Mitigation of financial, reputational, legal, and operational risk
- Continuity in the event of disaster or business disruption
- Protection of rights of our employees and the communities and individuals we serve
- Reduction of costs through greater business efficiency
- Protections and support in litigation
- Efficient use of employees' time
- 'Clutter-free', efficient working environment
- Employees and volunteers with appropriate skills for the digital workplace

3.0 Strategic Context |

3.1 SOSE's strategic planning framework recognises the importance and increasing level of collaboration partner agencies and other organisations, which takes place to deliver on the:

- Board's Operating Plan and the Regional Economic Strategy.
- SOSE's use of data and digital technology,
- how SOSE encourages workplace innovation, and
- how we benefit from a diverse and vibrant workforce reflects our Corporate Values and must all be considered and maximised.

3.2 Compliance with this Policy will help us meet the requirements and obligations of our external operating environment including:

- Compliance with statutory and regulatory obligations of all organisational functions, for example Health, Safety, Environmental legislation, and Financial and Procurement regulations
- Maintaining standards and membership of relevant professional bodies
- Contractual requirements with our public and private contractors and partners
- Effective, efficient, and compliant information sharing and partnership working

3.3 This Policy will enable us to comply directly with our information governance-related statutory obligations including:

- UK General Data Protection Regulation (UK GDPR)
- UK Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information (Scotland) Act 2002
- Privacy and Electronic Communications Regulations 2003
- Public Records (Scotland) Act 2011
- Payment Card Industry (PCI) Data Security Standard 3.1
- Equality Act 2010

3.4 SOSE Records Management Policy expects all SOSE corporate documents to be held within SharePoint, the SOSE electronic document and records management system (EDRMS).

4.0 Definitions |

4.1 Terms used within this policy have the following meaning in this particular context:

- Business Classification Scheme: Hierarchical model of the business functions and activities the authority undertakes, whether alone or in partnership
- Information Asset: A specific body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively. Information assets have recognisable and manageable value, risk, content, and lifecycles
- Information Asset Register: Maintained and controlled list of the information assets the organisation creates and maintains, and the governance rules under which they should be managed.

- Permanent Preservation: Continuous and indefinite preservation of records. For SOSE this means transfer of records to the National Records of Scotland who will manage the preservation.

- Records Management: The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of recorded information and the classification and management of information classified as records. This includes the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of that information classified as records.

- Retention Period: How long a category of information should be kept.

- Retention Schedule: A list detailing information types, the retention period for each along with the justification for each period, when that retention period starts and what the expected action is at the end of that retention period.

- Vital Records: The sub-set of information without which SOSE could not continue to function and which are deemed essential for purposes of business continuity.

- Information Asset Owner: The Information Asset Owner (IAO) is the senior manager accountable for the business function or activity to which the information assets relate. IAOs will generally be the head of the relevant business function, but there may be a limited number of exceptions where it is appropriate for a lower-level manager to be an IAO. IAOs may delegate some of their responsibilities listed below although will remain ultimately responsible for the information asset.

- Information Asset Custodian: The Information Asset Custodians (IAC) have an operational role, with a focus on delivery, support, and quality assurance. IACs will be supported by the Assurance and Resilience Business Partner and the Head of Governance and Assurance to fulfil their role. The IAC designation follows good practice and the organisational structure of the Records Management Plan.

- Senior Information Risk Owner: The Senior Information Risk Owner (SIRO) is accountable to SOSE's Chief Executive Officer for the management of the information risks across the organisation.

5.0 Scope |

5.1   This policy applies to:

- All SOSE employees, Board Members, external partners, or contractors and to anyone else who is authorised to create, access, share and use SOSE records and information

- All records and information generated, sent, received, or used by SOSE in the undertaking of its functions including service delivery, policy implementation, budget planning, meetings, and projects

- Records and information in all formats, systems and locations including paper records, electronic mail, word documents and spreadsheets, data in business systems, audio and video recordings and website and social media content

6.0 Policy Detail |

Policy Commitments

6.1   We recognise the value of our information and records as corporate assets, supporting our daily functions and operations and providing evidence of actions and decisions.

6.2   We ensure that adequate records are created and captured to account fully, transparently, and accurately for all actions and decisions.

6.3   We take appropriate action to protect the authenticity, reliability, integrity, and usability of our records as their business context and management requirements change over time.

6.4   We store, retrieve, and share information across the organisation effectively, efficiently, and securely including where they may be dispersed across different systems and locations.

6.5   We put in place procedures, processes, and controls to ensure that our information and records are kept safe, secure, and accessible for as long as they are required, regardless of their format or location.

6.6   We exploit the functionality of existing and planned IT systems and infrastructure to automate compliance with this policy to reduce staff burden of manual compliance and the risk of inconsistency and human error.

6.7   We manage personal data in compliance with data protection legislation. This policy and related procedures support that compliance as part of our wider Data Protection Policy.

6.8   We put in place appropriate governance controls around the sharing of information with our external partners and other third parties to enable effective joint working practice while at the same time minimising risks of inappropriate disclosure of personal, operational, or commercially sensitive information.

6.9   We will systematically and authoritatively dispose of information and records when they cease to be of business value.

6.10   We comply with any record keeping requirements resulting from our duties under Freedom of Information legislation and the Public Records (Scotland) Act, including the implementation of our RMP as agreed with the Keeper of the Records of Scotland, as data controller as defined by Data Protection legislation, and all other relevant legal, regulatory, and contractual obligations.

6.11   We take a proportionate, risk-based approach to the management of our information and records.

6.12   We develop and provide comprehensive and regular training to ensure that policy objectives are implemented effectively.

7.0 Policy Compliance and Governing Framework |

7.1   SOSE will meet these policy commitments in practice by establishing and maintaining the following information and records management standards, tools, and controls, proportionate to the risk and value of their related business activity or process:

- A business classification scheme to reflect the functions, activities, and transactions of the business
- An information retention and disposal schedule providing authoritative rules on what records we need to create and how long we need to retain them

- Destruction arrangements detailing the correct procedures to follow when disposing of business information

- An information asset register documenting the management requirements of all our information and records assets, based on their value and risk to the organisation

- Metadata schema, data quality standards and controlled vocabularies to aid information search and retrieval and an understanding of business context

- Incorporation of records and other information assets vital to the continuity of SOSE business in business continuity policy and plans

- Digital preservation arrangements (with NRS) in place for records required for long term or permanent retention to maintain their authenticity, accessibility, integrity, and usability over time

- Adequate processes and controls in place to meet the records management requirements of existing physical and IT systems

- Clearly documented records management requirements specified and delivered as part of any major change to IT systems and business processes

- Information security controls in place to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction

- The provision of adequate training as part of the corporate induction process for all new starts, and refresher training for existing staff, to ensure they are equipped to fulfil the records management responsibilities of their job role

8.0 Roles and Responsibilities |

8.1   The Director of Business Enablement has overall strategic responsibility for records management for ensuring SOSE meets its commitment to compliance with and effective operation of this Policy and the implementation of the organisation's Records Management Plan, supported by members of the Senior Leadership Team.

8.2   The Head of Governance and Assurance, Data Protection Officer has operational responsibility for records management liaising with the Director of Business Enablement, Senior Leadership Team, Management Teams and colleagues across all directorates as required. Key responsibilities include:

- Ensuring the maintenance, capture and recording of corporate data and information

- Managing information and records in line with the Public Records (Scotland) Act 2011 and other legislative requirements in addition to SOSE's own requirements

- Developing systems, delivering guidance, and influencing business processes to maintain the integrity of corporate data

- Providing access to and facilitating the sharing of records and information internally and externally

- Ensuring the availability and presentation of management information

- Delivering information management strategy, policy, and processes, including guidance and facilitation to increase awareness at all levels across the organisation

- Compliance reporting and performance monitoring and reporting

8.3   Information Asset Owners have responsibilities for the information within their scope of work. IAOs are responsible individuals involved in running the relevant business area. The IAOs must be aware of their responsibilities. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

8.4   All employees are responsible for the creation and capture of adequate business records related to the work that they do in line with this Policy, ensuring that records remain accessible and usable for as long as they are required to be retained under the SOSE Retention Schedule.

8.5   All Individuals must be able to justify what has been recorded and be prepared for that information to be released as part of data subject requests under Data Protection legislation, information requests under Freedom of Information legislation, investigation of complaints and evidence required by regulators, auditors and other relevant third parties.

9.0 Further Guidance |

9.1   Colleagues are referred to the Head of Governance and Assurance, Data Protection Officer, Assurance and Resilience Business Partner. and the IT and Digital Team, within the Business Enablement Directorate, for guidance relating to this Policy and for any guidance and support on issues relating to how records management practices can benefit SOSE.

10.0 Monitoring and Review |

10.1   SOSE will review this policy and procedure at least every two years or at times of significant legislative or organisational changes.