SDS Records Management Policy

Descriptor	Changes made	Date	Version
Policy first implemented	-	Feb 2014	1.0
Review no.1	Updated content	Feb 2015	2.0
Review no.2	Revised scope; reviewed/approved by IGSIG 22/01/2019	Jan 2019	3.0
Review no.3	Updated scope & policy statement; reviewed by IGLG 18/09/2020, updated for comments Reviewed and approved by Senior Dir Enabling Services	Dec 2020	4.0
Review 4	Clarified language and added definitions for technical terms. Substantive policy points remain the same. Submitted to DG, Feb 2023	Feb 2023	5.0
Review 5	Policy detail extended to explicitly cover leavers; 'what to keep where' section expanded	Dec 2024	

Name of policy being superseded (if applicable)	n/a
Related policies	SDS Freedom of Information Policy SDS Data Protection Policy SDS Policy on the Use of Protective Markings
Related SOPs	n/a
Related Guidance	Related process and guidance documents can be found in the Resources area of Connect, under **Records Management**
Equality Impact Assessment completed	No
Island Community Impact Assessment completed	No, as the policy is not likely to have an effect on an island community which is significantly different from its effect on other communities.
Intended Audience	All SDS colleagues
For publication	Internally only
Team responsible for policy	Business Systems
Policy owner contact details (email)	Kenny Parker
Policy due for review (date)	Dec 2026

Policies should have a clear purpose and perform at least one of the following functions. Please identify all the functions this policy performs.	**If statement applies, please mark with an X below**
Outline how we allocate limited resources to deliver services or outcomes	
Outline how SDS adheres to legislation, statutory duty etc.	
Ensure fair and consistent allocation of benefits	
Protect organisational assets, including data	X
Define expectations around the employee/employer relationship	
Other (please specify)	

Contents

1. Policy summary

The requirements for records management practices at SDS are presented, providing an explicit organisational commitment to the effective management of SDS information and records. It informs staff of their obligations throughout the time that information has value to SDS as well as of the importance of records management to achieving SDS's business objectives.

The policy applies to all information in all formats received, created, and maintained by all staff, regardless of grade, location, role or category of employment, in SDS.

2. Policy purpose and objectives

Routine use of good records management practices will mean that SDS's records are accessible, accurate, up to date, complete and secure as well as managed over their lifecycle. Doing this will bring business benefits to SDS and make it easier to comply with legislation.

The policy sets out good practice for creating, using, keeping and disposing of records. This will ensure that information at SDS is available to those with a need to access it for as long as the information has value to SDS and that the information is destroyed when it no longer has value to SDS.

SDS is committed to business excellence. This policy is meant to help SDS move from simply complying with legislation to having leading practices in its management of records.

3. Strategic context

Information is central to what SDS does and how it delivers its services. Good management of that information enables staff to work more effectively, promotes trust in SDS and reduces the risk of legal penalties while also saving time, effort, space, money and other resources.

Also, the law in the UK is placing much more emphasis on the need for good records management, with laws about freedom of information and data protection being two key examples of this.

Further, as a public body in Scotland, SDS must comply with the Public Records (Scotland) Act 2011 (the Act). This requires that SDS first develop and then maintain an approved records management plan (RMP), covering 15 different aspects of records management. SDS submitted its RMP to the NRS in early 2014. The NRS approved the plan, albeit with mandated improvements in some areas. This policy supports SDS's compliance with the Act.

SDS will develop and maintain an archiving agreement with the NRS regarding which categories of SDS records will be passed to the NRS for permanent preservation.

SDS is operating in a world offering many different platforms which all provide slightly different options for collaboration, presence and information storage functionality. SDS colleagues are reminded that there can be significant risks to SDS, its information and reputation if the wrong option is chosen. Where possible SDS will make use of the Microsoft 365 suite. SDS information must only be stored in approved platforms. SDS prefers for its data to be stored in the UK but allows for data to be stored in the EU subject to appropriate review. Other locations for data residency will be considered only in exceptional circumstances. Colleagues should seek advice when working with external partners and using their platforms. Advice on storing data out with the UK/EU, and the circumstances where this may be permitted, can be sought from the SDS Data Protection Team at **DPO@sds.co.uk**

4. Definitions

Some definitions relevant to records management are set out below:

National Records of Scotland (NRS) – The body that looks after public records in Scotland. Named in the PR(S)A, it provides advice and guidance on how to meet the provisions of the Act and assesses the RMPs produced by public bodies in Scotland.

Public Records (Scotland) Act (2011) (PR(S)A) – Public records legislation applicable in Scotland that mandates that public bodies keep proper records and document how those records will be managed through a records management plan (RMP). Implementation of the Act is overseen by the National Records of Scotland (NRS)

Records Management Plan (RMP) - Each public body is required by the PR(S)A to produce an RMP which details how the body will meet the expectations of the Act (as set out in a standard 'Model Plan'). An organisation's RMP is assessed by the NRS and each element rated red (failing), amber (acceptable on an improvement basis) or green (acceptable). An RMP can be approved with amber elements but not red. Once approved it is valid for 5 years.

Retention period – The length of time that a particular class or type of information will have value to SDS.

Retention Schedules – 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

5. Scope

The policy applies to all information in any format which SDS colleagues receive, create, keep or use as a part of their role at SDS. It is an explicit commitment by SDS to managing its records effectively.

This policy applies to all employees within SDS. Individuals who are seconded into SDS from another organisation (or employed through an agency) will be required to comply with this policy. Everyone involved in SDS business, including third party contractors and Board Members, has a responsibility to familiarise themselves and comply with this Policy.

6. Policy detail

It is SDS policy that:

- All information, no matter what format it is in (including emails and hardcopies) or platform it is stored on (e.g. MS teams, IShare, other SharePoint or business systems), must be managed over time by colleagues. This can be against the agreed retention period for that type of information or the approved retention schedule for a given system.
- SDS will automate the application of retention schedules across its business systems where it is possible and practicable to do so. This will prevent unmanageable collections of digital information being created.
- At the end of their retention period, files will be reviewed as per the Retention and Disposal Process.
- Colleagues must manage the SDS information they work with in a way that ensures that the information is appropriately available over the medium to long term. This means that:
    - Colleagues should save information on to the correct MS Team Site, section of IShare, other SharePoint site or relevant business system (see Section 7).
    - MS Outlook must not be used for more than short-term storage of information. Colleagues must manage their emails in line with the SDS Email Guidance; and
    - Other than the exceptions noted in Section 7, SDS information must not be shared from OneDrive (OD). When a file is ready to be shared save it to the appropriate collaboration space and send a link.
- Where colleagues create folder structures they should follow the guidance published on **Connect**.
- All information held within SDS's business systems (FIPS, CSS etc) must be managed in accordance with the approved guidance for each system.
- Colleagues involved in collaborations with external partners must follow the SDS External Information Sharing Policy.
- All third parties who create and/or hold records on behalf of SDS will have their obligations to manage those records included in their contract with SDS, covering information security, retention, disposal and legislative compliance.
- Hardcopy printing by colleagues should be kept to a minimum. Any that is created must be handled and disposed of according to its protective marking as per the **guidance published on Connect**.
- Colleagues should declare records in line with their service's expectations.
- Hardcopy records of value will be sent to offsite storage for the medium to long term.
- Prior to leaving SDS, colleagues will transfer all information of value to SDS from their OneDrive (OD) to IShare or relevant SharePoint site to ensure the appropriate continuity of access to the information.

Monitoring compliance with the policy will seek to use tools within Microsoft 365 and Power BI in the first instance.

7. Further guidance – what to keep where

A central requirement is to ensure that information is available to the colleagues that need to access it when they need to access it. This can be achieved by:

- Storing information in the right place i.e. in the right location on the appropriate platform
- Using file names and metadata that make it easy to find and identify the right file(s)
- Setting and then maintaining appropriate permissions.

Generally, information should be saved based on the topic or activity it is about and then by the type of information it is. E.g. all information about a specific project should be saved on the same platform and within the same part of the file plan. Within that file plan, the progress reports would sit together, the requirements documents would sit together and so on.

SDS's use of Microsoft 365 applications, including MS Teams for collaboration, is based on the concepts of 'my, shared and our' information to help determine which platform to use.

My information	i) Personal information about me and my employment at SDS. Save it in OneDrive (OD); and ii) Information about the employment of colleagues I am the manager for e.g. return to work forms. Information in either category can be shared directly from ODB, as an exception to the directive above, in order to preserve its confidentiality.
Shared Information	Either: i) Information being shared externally with partners through the SharePoint or MS Teams instance created for that and managed in line with the SDS External Sharing Policy. OR ii) Team admin and early drafts of documents that are being worked on. Material of generally short-term value to SDS. This could be created in IShare or sit within MS Teams
Our information	This is the business-critical information that SDS relies on. It might start out on different platforms but should be stored for the long term within the appropriate line of business systems or relevant IShare or other SharePoint file plan.

This has been illustrated on the DigiAye Hub on Connect with a **helpful infographic**

Output from MS Teams recordings and Copilot transcription of Teams calls will be saved to the OneDrive of the colleague who started the recording or transcription. This output will be deleted after 60 days. If a longer period is needed then the output should be as *Shared* or *Our* information, as in the table above.

Some ‘what to keep where’ do’s & don’ts

Do

- Save even draft documents directly into IShare (or other communal SharePoint), rather than One Drive. Allows colleagues to contribute early and make progress with it in your absence as well as allowing it to be managed properly
- Remind any colleagues leaving SDS to transfer any last form their OneDrive and or Outlook inbox to shared areas

Don’t

- share SDS information from your One Drive, with few exceptions it should not be there.
- leave everything in Outlook; keep your inbox tidy for ease of use, increased productivity and fewer compliance problems.

Understanding how MS Teams is being used across SDS continues to develop. Updated guidance and a range of case studies will be provided to support colleagues make the most of what Microsoft 365 has to offer while still following good records management practices.

The policy detail will be reviewed every two years to ensure that it continues to meet SDS’s needs.

Colleagues are referred to **Connect** for guidance on naming documents, using search in IShare, creating folder structures and other practical aspects of records management