Information and Records Management Policy

Document type:	Policy		
Document number:	IT-088	**Version**	02
Department:	Information Technology		
Approved by:	Executive Board		
Date approved:	12/05/2025	**Review Date**	12/05/2028
Publication:	SOAS website		
Related Documents:	• SOAS Records Retention Schedule • SOAS Data Protection Policy • SOAS IT Acceptable Use Policy		

Note: All policies must be read in conjunction with all other SOAS policy, procedure and guidance documents. Printed copies of policies may not be the most up to date, therefore please refer to the policy pages on the SOAS external website or intranet for the latest version.

1. Introduction

1.1 The University recognises that the efficient and effective management of its unstructured information and records is necessary to support its core functions and activities, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution.

1.2 It is also recognised that the University, in common with most other organisations, is seeing an exponential increase in the volume of digital files being created and stored on its systems, posing a challenge for traditional records management approaches, as it is more difficult to ensure that the key characteristics of a record are preserved and protected when the record does not have a physical existence. Sound policies, procedures, and practices for managing information and records, based on the latest good practice are critical if we are to successfully address this challenge.

1.3 This policy sets out the principles that support the University in discharging its obligations in this area and makes provision for the management of records at the different stages of their lifecycle.

1.4 By adhering to this policy, the University will be able to manage its records in a way which:

- Facilitates compliance with statutory and regulatory requirements
- Prevents unauthorised or unlawful disclosure of information by ensuring records are managed in a controlled way
- Protects the rights and interests of SOAS, its staff, students and other stakeholders by maintaining high quality information for as long as its required, and to ensure its timely and secure destruction

- Supports continuous improvement in the University's core activities of teaching and research, and evidence-based decision making by maintaining accurate and reliable records
- Provides evidence of good corporate governance, transparency and accountability
- Supports business efficiency and continuity by ensuring information can be quickly located and protecting vital information for the continued functioning of SOAS during a disaster
- Provides evidence in litigation
- Maintains SOAS's corporate memory by securing records of historical significance.

2. Scope

2.1 This policy applies to all SOAS records, regardless of how they were created and how they are stored (for example, whether hard copy or digital; held by individuals or in centralised systems), and covers the entire lifecycle of records, from creation through to disposal.

2.2 This policy applies to 'all staff' creating and maintaining records as part of their SOAS role.

2.3 For the purposes of this policy, 'all staff' includes the following, whether remunerated or not:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with (i.e. performing services for or on behalf of) the University (for example, agents and consultants)

2.4 Except where the terms of funding take precedence, this policy will also apply to all records of research generated by SOAS staff.

2.5 Except where a student is also 'staff' of the University, or creating and maintaining records as a part of the University's functions (e.g. as part of research work), this policy does not apply directly to students.

3. Definitions

Record	A record is a subset of recorded information which supports and shows evidence of SOAS activities. It can exist in any format and be created or received by SOAS or individual members of staff. Examples can include final reports, emails confirming an action or decision, spreadsheets showing budget decisions, photographs or maps of field missions, which need to be kept as evidence.
Information	Information is any data, facts, or knowledge that can be communicated or processed, irrespective of medium, but often contained in a file format. Information sources are often "non-records": they are useful but do not provide evidence in the same way as records. Common examples include drafts, notes, lists, most emails, structured datasets, reference materials or items published by organisations other than SOAS.
Records Management	Records management helps us to tell when a piece of information is also a record. It aims to ensure that we create the records we need, keep these records in ways that allow for efficient access and use, maintain records for as long as we need them for operational, legal, and audit purposes, and to dispose of them when they are past their retention period.
Records lifecycle	This is a model used by records managers to describe the stages through which a record progresses during its existence. It is helpful for planning records management activities, so that records can be maintained and stored efficiently.
Disposal	The decision and process by which a SOAS record is either destroyed or transferred to the custody of the University Archive for permanent preservation. Most records are destroyed at the disposal point; however a small percentage of records is identified on the Records Retention Schedule as having permanent value to the University.
Archiving	Archiving in the context of records management refers to the professional management of those records that have been identified for permanent preservation because of their administrative, informational, legal and historical value as evidence of official business of the University and transferred to the University Archive. It does not simply refer to secure cold storage. Archives are a small but important subset of the University's official records.
Retention Schedule	This is a policy setting out what records SOAS holds and how long they will be retained before disposal. It can also be used to set out what needs to happen to records at different stages of their lifecycle to ensure that they are stored efficiently. To view the schedule, please see SOAS Retention Schedule
Vital Records	Specific records without which SOAS could not function, and which would be impossible or prohibitively difficult to reconstruct in the event of a disaster.

4. Roles and Responsibilities

4.1 **All Staff** are responsible for familiarising themselves with and adhering to this policy and the Records Retention Schedule when creating and maintaining records as part of their work for the University.

4.2 **Executive Board** has delegated responsibility on behalf of the Audit & Risk Committee to ensure that the University complies with best practice standards for the governance of information and records, which will be set out by this policy which they oversee and approve.

4.3 **College Deans and Directors of Professional Services** are responsible for:

- Ensuring that staff in their area are aware of this policy and their responsibilities
- Ensuring that records belonging to their College or directorate are created, maintained and disposed of in accordance with this policy and the Records Retention Schedule.
- Encouraging and promoting a culture of good records management within their Directorate or College.

4.4 **The Information Compliance Manager** has overall responsibility for Records Management. Operational responsibility is delegated to the Records Manager and Archivist who is responsible for developing the corporate records management policy, procedures, and guidance, promoting good practice and promoting compliance with the policy and procedures, and managing the University Archive collection.

4.5 **Local Information Champions** are responsible for communicating records management policy and procedures to their directorates and reporting on their implementation to the Records Manager and Archivist.

4.6 **The Information and Technology Directorate** is responsible for:

- Providing and maintaining technology which will support the University in complying with this policy
- Providing an off-site storage service for hard copy records.
- Providing secure disposal services for IT hardware

4.7 The **Estates and Facilities Directorate** is responsible for providing secure local onsite storage for physical records, where required, and providing onsite confidential waste disposal services.

5. Policy

5.1 Six Records Management Principles

5.1.1. **The record is created and held:** the information the University needs to evidence and reconstruct the relevant activity or transactions is recorded and is accurate.

5.1.2. **The record can be accessed:** when it is needed, it is possible to discover, locate and access the information. It is possible to present it in a way that is true to the original presentation of the information. The authoritative version can be identified in cases where multiple versions exist.

5.1.3. **The record can be interpreted:** The context of the record can be established: who created the document and when, during which business process, and how the record is related to other records.

5.1.4. **The record can be trusted:** the information and its representation in the record is fixed and matches that which was actually created and used, and its integrity, authenticity and provenance can be demonstrated beyond reasonable doubt.

5.1.5. **The record can be maintained through time**: the structural integrity of the record can be maintained for as long as the record is needed (in line with the Records Retention Schedule, and in some cases permanently), notwithstanding transfers to other agreed locations, systems, formats and technologies so that it remains present, accurate, trustworthy, interpretable and accessible.

5.1.6. **The value of the record is understood and protected:** it is recognised that our records form part of our corporate memory and are an important institutional resource which must be protected across their lifecycle in accordance with the above principles. A record has a single Owner, even when used or accessed by multiple teams.

5.2. Records Retention Schedule

5.2.1. The Retention Schedule applies to the primary or master copy of a record (especially if there is more than one copy held by different departments).

5.2.2. The Schedule will be maintained and developed with reference to sector models and best practices, such as the Jisc model retention schedule and classification scheme.

5.2.3. The Schedule will be reviewed by the Records Manager and Archivist every five years.

5.2.4. Guidance and training will be made available to support staff in the appropriate use of the Retention Schedule.

5.3. Records Creation and Maintenance

5.3.1. Records must be maintained and stored in such a way that they can be easily identified and located to support business activities and that ensures appropriate accountability, using established procedures for secure access and handling, including via use of appropriate and approved cloud storage platforms, such as those available in our Microsoft365 tenant.

5.3.2. Where the University procures or develops IT, collaboration and/or business systems, records management requirements must be considered, documented and addressed from the initial requirements stage.

5.3.3. Full and accurate documentation of IT and record-keeping systems should be maintained by the owning department. This includes ensuring that records which are essential to business continuity (‘vital records’) are identified and protected as part of Business Continuity Plans.

5.3.4. Appropriate technical and organisational measures will be employed to safeguard the security and integrity of University records and provisions made (i) to maintain their reliability, integrity and preservation during their lifespans and (ii) to prevent the unauthorised or unlawful use, disclosure or loss of information.

5.3.5. Guidance will be made available to SOAS staff, including guidance on such matters as security and access to records, document naming and version control, and appropriate storage at different stages of the records lifecycle.

5.3.6. Staff will receive training in records management appropriate to their role.

5.3.7. Records and information management risks will be identified in the University’s Risk Register.

5.4. Disposal

5.4.1. Guidance and facilities for the appropriate disposal of records will be provided.

5.4.2. Where systems and applications are to be decommissioned or records are scheduled for migration or conversion between business/record systems, including conversion to digital formats, the Records Manager should be consulted.

5.4.3. The decommissioning of digital services and digitisation should be carried out in line with IT Services’ and Records Management guidance and the Records Management Principles.

5.4.4. The ability to appropriately dispose of records according to their retention period should be built into systems wherever possible.

5.5. Archiving

5.5.1. Records identified for permanent preservation by the Retention Schedule should be transferred to the University Archive in coordination with the University Archivist.

5.5.2. Permanent archival records should not be stored locally.

5.5.3. Advice should be sought from the Archivist if there is uncertainty about the longer-term value of a record.

5.6. SOAS records and encrypted instant messaging platforms

5.6.1. SOAS mandates the use of its own business systems for the conduct of its business and the management of the records created therein.

5.6.2. It is recognised that there will be exceptional circumstances where the use of certain instant messaging platforms may be necessary, including out of hours incident management and emergency communications with students and staff where access to SOAS online systems poses a challenge due to local restrictions or a natural disaster, or other state of emergency.

5.6.3. SOAS will provide guidance and support to staff on the most appropriate use of such platforms.

5.7. SOAS records generated by AI

5.7.1. Records which are being relied on for institutional decision-making and which have been generated or co-generated by artificial intelligence must be labelled accordingly to allow the University to verify the authenticity and integrity of such records.

5.7.2. Records which are generated or co-generated by artificial intelligence must not be relied on as sources of truth without scrutiny by appropriate SOAS staff with knowledge of the subject matter.

5.7.3. The member of staff deploying AI to generate or co-generate records is accountable for their accuracy, and for ensuring this activity aligns with SOAS' ethical approach to AI

6. Conditions

The following laws, regulations, codes of practice, standards and policies are part of the legal and professional framework which has a bearing on this policy.

6.1. Laws and regulations

- UK General Data Protection Regulation and Data Protection Act 2018
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Limitation Act 1980

6.2. Standards and Codes of Practice

- BS ISO 15489-1:2016, Information and documentation – Records management – Part 1: General
- BS ISO/IEC 27001: 2005, Information technology. Security techniques. Information security management systems. Requirements
- BS ISO/IEC 27002: 2005, Information technology. Security techniques. Information security management systems. Code of Practice
- BS 10008 Evidential weight and legal admissibility of electronic information - Specification
- BS 8470:2006, Secure destruction of confidential material. Code of practice
- BS 4783, Storage, transportation and maintenance of media for use in data processing and information storage
- Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000
- JISC Higher Education Business Classification Scheme and Records Retention Guide.