Records Management Procedure	
Enabling Policy Statement; Executive Owner. Approval Route:	Our Data – University Secretary and General Counsel
Associated Policy Statements:	Our Data – University Secretary and General Counsel
Authorised Owner:	University Data Protection Officer
Authorised Co-Ordinator:	University Data Protection Officer
Effective date:	02/12/2024
Due date for full review:	3 years
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	New Procedure	Compliance Data Committee	02/12/2024

1. Purpose

The University recognises that the efficient management of records is necessary to support evidence of its core functions, to comply with the law, to meet accountability requirements and stakeholder expectations, and to enable the effective management of the institution.

1.1. This procedure sets out how to ensure the creation, maintenance and protection of authentic, reliable usable data and records, within the University. It establishes a framework and accountabilities for information and records management, through which best practise can be implemented and audited.

1.2. The University has a statutory obligation under the Data Protection Act 2018, UK General Data Protection Regulation 2016/079 and the Freedom of Information Act 2000, to maintain accurate records of its activities and to plan for their safe keeping and secure disposal. All records created during the University's business are public records.

2. Scope and Exceptions to the Procedure

2.1. This procedure applies to all recorded information in digital and hard copy formats that is created, received, and maintained by staff as information users while carrying out their university functions. Records are those documents, regardless of format, which facilitate university activities and operations, and which are thereafter retained to provide evidence of its transactions or activities.

2.2. This procedure applies to records crossing the course of research, whether internally or externally funded, in addition to any contractual and academic record-keeping requirements.

2.3. This procedure covers all applications and business systems used to create, manage, and store university information and records, including content and information management systems, databases, e-mail, voice and instant messaging, websites, and social media applications. The procedure covers information created and managed in-house and off-site including cloud-based platforms.

2.4. This procedure is binding on those who create or use university records, for instance information users such as university staff, students, associates, partners, contractors, and visitors whether accessing records on or off campus.

3. Definitions and Terminology

3.1. **General Data Protection Regulation** – is a set of EU rules on data protection and privacy.

3.2. **Data Protection Act 2018** – is the UK's implementation of the General Data Protection Regulation (GDPR)

3.3. **Data Protection Impact Assessment (DPIA)** – is an assessment of the impact of the processing operations on the protection of personal data.

3.4. **ISO15489** - is an international standard for the management of business records, consisting of two parts: Part 1: Concepts and principles and Part 2: Guidelines.

3.5. **Records** - recorded information, in any form, creative received and maintained by the university in the transaction of its business or conduct or affairs and captures evidence of such activity.

3.6. **Senior Information Risk Owner (SIRO) –** plays the main role in the management and protection of the University's information assets.

3.7. **Data Protection Officer -** monitors and review the University's compliance with applicable legislation, regulation, and standards.

3.8. **Corporate Records** - Records that relate to the corporate business of the university. i.e., including but not exclusive.

- Corporate governance and assurance activities, for instance, committee minutes, action logs, risk registers, policy framework
- Staffing personnel activities i.e., HR
- Health and Safety/Facilities Management
- Financial management and accounting
- Procurement and contracting activities
- Press/media enquiries

3.9. **Electronic Record** - an electronic record is an electronic document which has been formally declared as a corporate record. A typical electronic record consists of both electronic content and metadata. While electronic documents can be edited and deleted, electronic documents are held in a fixed state, with appropriate access applied.

3.10. **Records Management** - a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage, and disposal of records, in a way that is administratively and legally sound. The key components of records management are:

- Record Creation
- Record Keeping
- Record Maintenance
- Access and disclosure
- Closure and transfer
- Appraisal
- Archiving
- Destruction

3.11. **Records Lifecycle** - the life of a record from its creation/receipt through the period of its current (active) use, then into a period of semi-current (inactive) retention such as closed files which may still be referred to occasionally and finally either destruction, discussion, or archival preservation. Records management procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage, and records audit.

3.12. **Folder** - a folder is a container for related records/folders segmented into parts which are the primary unit of management and may contain one or more records or markers where applicable.

3.13. **Naming Convention -** a naming convention is a collection of rules which is used to specify the name of the document, record, or folder.

3.14. **Classification -** A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.

3.15. **Protective Marking -** Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.

3.16. **Disposal** - The manner in which a record is disposed of after a period of time. It is the final stage of record management in which a record is either destroyed or permanently retained.

3.17. **Users (end users)** - This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much of the material which constitutes the record. Since records systems tend to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.

3.18. **Executive Owner** - University Secretary and General Counsel

3.19. **Authorised Owner** – Data Protection Officer

4. Procedure Principles

4.1. All records that sit under the Procedure of Policies and Procedures Framework (POPP) should follow the requirements of that framework. This will include policies, procedures, codes of practice and other guidance documents.

4.2. The University will manage records and data efficiently and systematically following the standards as set in ISO15489 and the statutory code of practise for records management, to support university operations including regulatory, funding, and ethical requirements. All information management practises in the University should align to this procedure and its supporting procedures.

4.3. Records will be created, maintained, and retained to provide information about and evidence of the university's decisions, transactions, and activities. Appropriate systems will be in place to record these decisions and activities.

4.4. Records must be maintained in line with these six records management principles to ensure their viability and quality across their lifecycle:

- **the record is present**: the information the University needs to evidence is recorded and is accurate.
- **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.
- **The record can be interpreted**: a context for the information can be established, showing when, where and who created it, how it is related to other records, and what process/activity it comes from.
- **Record can be trusted**: the information and its representation are fixed and matches that which is created and used, and its integrity, authenticity and provenance can be demonstrated beyond reasonable doubt.
- **The record can be maintained**: can be accessed, interpreted, and trusted for as long as it is needed in line with record schedules 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.

- **The record's value is understood and protected**: it is recognised that our records form part of the corporate memory and our important institutional resource which must be protected across their lives.

4.5. When university departments procure or develop IT and business systems, records management requirements must be considered, documented from the initial requirement stage. A data protection impact assessment must be undertaken for new digital systems and services to help assess their ability to function as a record keeping system and the data protection officer services consulted for advice.

4.6. Departments and services must maintain full and accurate records of their records, and keep systems and processing of personal data in information asset registers. This includes ensuring that records which are essential to business continuity are identified and protected.

4.7. Appropriate measures will be employed to safeguard the security and integrity of university records and provisions made:

- to maintain their reliability, integrity, and preservation during their lifespan
- to prevent the unauthorised or unlawful use, disclosure, or loss of information

4.8. Records must be maintained and stored in such a way that they can be easily identified and located to support business activities and the issuers appropriate accountability, using established procedures for secure access and handling.

4.9. Records will be retained and disposed of in accordance with agreed retention schedules in a controlled and compliant manner. Retention schedules will set out the minimum period that a record should be retained and will be reviewed regularly and amended as necessary. Retention schedules must be agreed by the information asset owners for the relevant university function. When the retention period of records expires, the records will either be destroyed or, if they have lasting historical value, transferred to the University archive.

4.10. Where systems or applications are to be decommissioned or records are scheduled for migration or conversion between business/record systems, including conversion to digital formats, the information governance team should be consulted. 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.

4.11. A small percentage of university's records will be selected for permanent preservation if appropriate by the relevant information asset owner or head of department. These records will become part of the university archive which maintain the university's corporate memory by preserving records of enduring evidential and historical significance.

4.12. Information and records management awareness and training will be provided to staff by the information governance services where required.

Roles and Responsibilities

4.13. All staff and information users are responsible for creating, maintaining and preserving accurate records that support and document their activities in accordance with this procedure and its associated policies, procedures, and guidance. They must know what information they hold, where it is held and complete records management training.

4.14. Information asset owners are responsible for ensuring that all records in their area are managed in conformance with this procedure and associated policies and procedures. Information asset owners

are responsible for promoting this procedure and ensuring their staff complete mandatory data protection training.

4.15. Information governance services is responsible for promoting and supporting compliance with this procedure across the university and its wholly owned subsidiaries, including development of retention schedules and procedures, drawing up guidance and providing training and support on good information and records management practice.

4.16. The University owns all records created by its employees carrying out university related functions and activities unless otherwise specified under contract or in its regulations.

4.17. Staff, students, partners, consultants, and visitors who act in breach of this procedure, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Oversight

4.18. The University Secretary and General Counsel, as Senior Information Risk Owner (SIRO), has overall responsibility for records management within the university. The Compliance Data Committee is responsible for the oversight of data compliance and risk management, and the approval and monitoring of related procedures, including this Records Management Procedure.

Record Creation and Classification

4.19. Record creation is one of the most important processes in records management and all staff within the organisation should aim to create good records that can be used in an effective manner.

4.20. It is important that records are kept in context and the best way to achieve this is to 'file' or 'classify' them. Records cannot be tracked or used efficiently if they are not classified or have been classified inappropriately.

4.21. Records captured or filed in a corporate filing system must be regarded as authentic or reliable. A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily (e.g., standard naming convention[1] and version control). Where appropriate, documents should be given a review date (e.g., corporate policies).

4.22. To ensure quality and continuity of operational services, all records should be kept accurate and up to date. All University staff who are responsible for recording information in both paper and electronic format must ensure they fully understand their responsibilities as set out in this procedure and remember that records may be used in a court of law.

4.23. The aims of the University's Records Management System are to ensure that:

- **The correct records are readily available when needed** – so that staff are able to access information when needed (as appropriate) and that the organisation is able to form a reconstruction of activities or events that have taken place. Records, and the information within them, should be located and displayed in a way consistent with their use, and the current version should be clearly identifiable where multiple versions exist.

- **Records can be interpreted** - the context of the record should be easily understood. It is important

[1] A naming convention is a common set of rules or guidelines to apply to the naming of electronic records. Staff should give a unique name to each record which is meaningful and reflects the record's content. Naming should be similarly structured where records are linked (e.g., previous versions).

that records clearly demonstrate who created or added to the record and when, during which business process, and how the record is related to other records.

- **Records can be trusted** – the record reliably represents the information that was used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation, and trustworthiness can be maintained for as long as the record is needed, despite changes of format.

- **Records are secure** – records are protected from unauthorised or inadvertent alteration or erasure and that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required**.**

- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures which are in line with the requirements of the JISC Records Retention Management.

- **Staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

Records Maintenance and Storage (Electronic and Hard Copy Records)

4.24. All staff (as defined within the scope of this procedure) have a duty for the maintenance and protection of records they use or create.

- Referencing
  Each Faculty should establish and ensure compliance with a document referencing system that meets its business needs and is easily understood by staff members that create, file, or retrieve records held in any media. Several types of referencing can be used, e.g., alpha-numeric, alphabetic, numeric or keyword.

  The most common of these is alpha-numeric, as it allows letters to be allocated for a business activity, e.g., HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the records are kept and identify the record by reference to date and format.

- Naming
  Each Directorate should nominate staff to establish and document file naming conventions in line with national archives advice, i.e.
  - Give a unique name to each record.
  - Give a meaningful name which closely reflects the records content.
  - Express elements of the name in a structured and predictable order.
  - Locate the most specific information at the beginning of the name and the
  - most general at the end; and
  - Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

- Security Classification
  Emails and documents containing sensitive information (e.g., information that could have damaging consequences if it were lost, stolen, or published in the media) should be marked as "Restricted." Such documents include the University incident Response Plans; or documents relating to the University's response to a major incident.

  Indexing and Filing
  Each Directorate should establish and document a clear and logical filing structure that aids retrieval of records.

  The register or index is a signpost to where paper corporate records are stored, (e.g., the relevant folder or file), however, it can be used as a guide to the information contained in those records. The register should be arranged in a user-friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear logical names that follow the University's naming convention.

  The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. Filing of corporate records to local drives on PCs and laptops is not appropriate. Files must be saved to the departmental network/SharePoint site, to ensure only authorised access is available and that appropriate backups are taken.

  Likewise, the filing of key organisational paper records in desk drawers is not appropriate, departmental accessible secure storage should be used.

  Version Control
  A system of version control must be implemented to enable staff to know that they are working on the latest/correct version of the documentation. This may be in the form of a version number and date or by use of document creation date.

4.25. The identification and safeguarding of vital records is necessary for business continuity and will be included as necessary in business continuity plans.

4.26. It is important that the University has robust 'tracking and tracing' procedures to provide an audit trail of the movement and location of records. The University will maintain an information asset register that clearly identifies business critical information assets (in relation to both electronic and hard copy records) and the safeguards and controls in place to protect them.

4.27. Records containing person identifiable data or corporate sensitive information must be stored securely in accordance with Data Protection Act 2018.

4.28. The movement and location of paper records should be controlled to ensure that a record can easily be retrieved at any time.

4.29. Final versions of corporate records will be included on SurreyNet to ensure that all staff can have access to the approved versions of policies and corporate documents. Policies and Procedures documents that meet the requirements of the Freedom of Information Act 2000 will be published on the University website Policies and Procedures page.

4.30. The records storage areas must comply with health and safety and fire regulations and be considered in accordance with any confidentiality and access issues.

4.31. Once records have reached their semi-current (inactive) state they are to be transferred to the University records store in accordance with the Access Procedure.

Retention and Destruction Schedule

4.32. It is a fundamental requirement that all of the University's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the University's business functions.

4.33. Keeping unnecessary records uses up valuable space and can incur unnecessary costs. It can also cause problems when trying to retrieve important information, for example, when servicing a request made under the Freedom of Information Act 2000.

4.34. The University will adhere to the retention and disposal periods as set out in the JISC Records Retention Management Schedule.

4.35. When a record is deemed to have no further value to the University or has reached its assigned retention period, it should then be reviewed and if necessary, destroyed under confidential destruction conditions (as per the disposal actions set out in the JISC Records Retention Management Schedule).

4.36. A local retention and disposal schedule for any records which are not listed in the current version of the JISC Records Retention Management Schedule will be agreed by the University's Compliance Data Committee.

4.37. All records which are to be disposed of must be destroyed in a secure manner to ensure the information is illegible and irretrievable.

4.38. It can be a criminal offence to destroy information; therefore, the organisation needs to be able to clearly demonstrate that records destruction has occurred appropriately.

4.39. Records that need to be preserved for their archival value should have a clearly documented rationale for keeping beyond their scheduled disposal date. Some records will qualify for archive and should be transferred to the University Library.

4.40. Information Governance services will hold a central record of documents that have been destroyed under this procedure and any records that require keeping beyond their scheduled disposal dates. The record will include the document reference, description, and date of destruction.

4.41. Further advice and guidance in relation to any of these points can be obtained from the Information Governance Department at dataprotection@surrey.ac.uk

5. Governance Requirements

5.1. **Implementation: Communication Plan**

- Campus wide communication of this Procedure is required. This Procedure will be published on the University Policies and Procedures webpage. Further information will be included on the Information Governance SurreyNet pages.

5.2. **Implementation: Training Plan**

- The Information Governance team will offer training as and when required in support of this

procedure on the SurreyNet pages. Overall training will be provided via the mandated data protection training.

5.3. **Review**

- This Procedure will be reviewed every three years and monitored by the Compliance Data Committee.

5.4. **Legislative Context and Higher Education Sector Guidance or Requirement**

- UK General Data Protection Regulation 2016/679
- EU General Data Protection Regulation 2016/679
- Data Protection Act 2018
- Human Rights Act 1998
- The Common Law Duty of Confidentiality
- ICO Accountability Framework
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Freedom of Information Act 2000
- ISO15489-1:2016 – Information and Documentation (Records Management)
- JISC Records Retention Management
- NHS England Data Security and Protection Toolkit

5.5. **Sustainability**:

The sustainability impact of records management is considered with the core business requirement of the management of records to reduce the creation and management of paper records and transfer to electronic processing.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 02/04/2024 and is held by the Authorised Co-Ordinator.

6.2. This procedure sets out how to ensure the creation, maintenance and protection of authentic, reliable usable data and records, with appropriate evidential characteristics, within the University. It establishes a framework and accountabilities for information and records management, through which best practise can be implemented and audited. Consultation has taken place with:

Stakeholder	Nature of Engagement	Request EB Approval Y/N	Date	Name of Contact
Chief Information Security Officer	Consultation			Tom Brown
Equality and Diversity Advisor	Consultation			Michael Hassell
Archives and Special Collections Manager	Consultation			Helen Roberts
Head of Governance Services	Consultation		01/11/2024	Ros Allen
Head of Sustainability	Consultation			Martin Wiles
Director of Health and Safety	Consultation		07/11/2024	Matthew Purcell
Academic Freedom / Freedom of Speech	Consultation		13/11/2024	Abigail Bradbeer

GRA [POPP]	Consultation		21/11/2024	Kelley Padley