Data Retention Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Is the Procedure for internal use only (Non-disclosable)?	Disclosable
Associated Policy Statements:	-
Authorised Owner:	University Data Protection Officer
Authorised Co-ordinator:	Head of Governance Services
Effective date:	18/12/2025
Due date for full review:	18/12/2028
Sub documentation:	JISC Records Retention Schedule

Approval History

Version	Reason for review	Approval Route	Date
1.0	New Procedure	Compliance (Data) Committee	18/12/2025

1. Purpose

1.1. Under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR), the University is classed as a controller. To ensure that it complies with data protection legislation the University has appointed a Senior Information Risk Owner (SIRO) - this is assigned to the University Secretary and General Counsel - and a Data Protection Officer (DPO) and they have oversight of the detail of this procedure.

1.2. The University recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the institution. Information held for longer than is necessary creates additional risk and cost, and breaches data protection principles.

1.3. Effective and adequate records, and data management is necessary to:

- Ensure that the University conducts itself in a structured, efficient and accountable manner.
- Reduce the risks associated with personal data and provide continuity in the event of a disaster or security incident.
- Ensure that the University realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems.
- Support University functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes.
- Meet legislative, statutory and regulatory requirements.
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner.
- Assist in document policy formation and managerial decision making.
- Protect personal information and data subject rights.
- Avoid inaccurate or misleading data and minimise risks to personal information.
- Erase data in accordance with the legislative and regulatory requirements.
- Ensure that records of historical value to the University and to the wider public are transferred to the University Archive.

2. Scope and Exceptions to the Procedure

2.1. This procedure is in place to ensure all staff (including temporary, contractors and subsidiaries), visitors and students are aware of their responsibilities in relation to the University's approach to data retention and deletion and how it complies with the core principles of data protection.

2.2. The purpose of this document is to provide University of Surrey's statement of intent on how it provides a structured and compliant data and records management system that facilitates the University's activities and provide evidence of transactions and functions.

2.3. Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

2.4. This procedure applies to all staff within the University of Surrey and the subsidiaries. Adherence to this procedure is mandatory and non-compliance could lead to disciplinary action.

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. **JISC Retention Schedule –** provides guidance on how long information should be retained in higher and further education institutions. It includes recommended retention periods to help organisations draft their own schedules.

3.9. **Stag Hill House Records Store –** the records store holds paper records under the control of the information governance department. Access to and to store records go to dataprotection@surrey.ac.uk

3.10. **Archival Value** – a secondary, historical value inherent in the information content of a record, distinct from the original business purposes for which the record was created.

3.11. **Archiving** – the act of designating records as requiring indefinite retention on the basis of their archival value, and the ongoing management and preservation of said records as a distinct information resource.

3.12. **University Archive** – the official corporate archive of the University, managed as primarily a heritage resource of use to both the University and the general public. The University Archive is managed by Archives & Special Collections within the University Library – archives@surrey.ac.uk.

4. Procedural Principles

4.1. 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.

4.2. The University needs to collect personal information about the people it employs, it works with, its students and the people it has a business relationship with, in order to carry out its business functions and activities, and to provide the products and services defined by our business type. This information can include (but is not limited to), name, address, email address, data of birth, IP address, identification number, bank details, confidential information, and sensitive information.

4.3. In addition, the University may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. The University is committed to collecting, processing, storing, and destroying all information in accordance with UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information the University process and store.

4.4. The University ensures it complies fully with the storage limitation principle as defined by Article 5 (1)(e) of the UK GDPR:

4.4.1. *"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')."*

Objectives

4.5. It is the University's objective to implement the necessary data retention procedures and systems which assess and manage the following processes:

- The creation and capture of records.
- Compliance with legal, regulatory, and contractual requirements in relation to record retention standards.
- The storage and security of records in support of statutory requirements.
- The protection of record integrity and authenticity during retention.
- The use of records and the information contained therein.
- Access to and disposal of records.

4.6. Records contain information that are a unique and invaluable resource to the University and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals the information refers to. This equally applies to records that are retained for permanent retention.

4.7. The University's objectives and principles in relation to data retention are to:

- Ensure that the University conducts itself in an orderly, efficient, and accountable manner.
- To only retain personal information for as long as is necessary.
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review, and destruction of information.
- Support business functions and providing evidence of compliant retention, erasure, and destruction.
- Ensure the safe and secure disposal of confidential data and information assets.
- Comply with the relevant data protection regulations, legislation, and any contractual obligations.
- Ensure that records and documents are retained for their legal, contractual, and regulatory period stated in accordance with the rule or terms of each body.
- Ensure that no document is retained for longer than is legally or contractually allowed.
- Ensure that records of historical value to the University and to the wider public are transferred to the University Archive

Guidelines & Procedures

4.8. The University manages records efficiently and systematically, in a manner consistent with data protection requirements, and this procedure is widely disseminated to ensure a standardised approach to data management, retention and deletion.

4.9. Records will be created, maintained and retained to provide information about, and evidence of University transactions, customers, employment, and activities.

4.10. Retention schedules will govern the period that records will be retained. These schedules will be actioned and retained by relevant departments; the data protection team will also hold these schedules.

4.11. It is the University's intention to ensure that all records and the information contained is:

- Accurate
- Accessible when necessary
- Complete
- Compliant
- Reviewed
- Secure

Retention Period Protocols

4.12. All records retained during their specified periods are traceable and retrievable. All University student and employee information is retained, stored and destroyed in line with JISC Retention Schedule and regulatory guidelines.

4.13. For all data and records obtained, used and stored, the University will carry out periodic reviews of the data retained, checking the purpose of use, continued validity, accuracy and requirement to retain.

4.14. Where it is not possible to define a statutory or legal retention period, the University will make a business decision, in line with data protection principles, by which a period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices. Any amendments to the approved local retention periods must be approved between the University Data Protection Officer and relevant Information Asset Owner and included in the local data retention schedule held by the Data Protection Officer.

4.15. Processes will be in place to ensure that records pending audit, litigation or investigation are not destroyed or altered. This process is called a "Legal Hold" approved only by the legal team.

Retention and Destruction Schedule

4.16. 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.

4.17. 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 or Data Protection Act 2018.

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

4.19. 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, disposed of as per the disposal actions set out in the JISC Records Retention Management Schedule. Disposal may take the form of secure destruction or archiving.

4.20. 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.

4.21. Destruction of records must be carried out in a secure manner to ensure the information is illegible and irretrievable.

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

4.23. Records that need to be preserved for their archival value should have a clearly documented rationale for keeping beyond their scheduled disposal date. Archived records may be transferred to the University Archive, or continue to be managed for business purposes by their designated owner. (Note that in the latter circumstance, the 'archiving purposes in the public interest' exemption of the Data Protection Act 2018 is unlikely to apply).

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

University Archive

The University Archive is the official corporate archive of the University, managed by Archives & Special Collections within the University Library. It is managed as primarily a heritage resource of use to both the University and the general public. The processing of personal data within the University Archive is permitted under the 'archiving purposes in the public interest' exemption of the Data Protection Act 2018. Personal data within the University Archive is managed in accordance with The National Archives Guide to archiving personal data (2018) and other archive sector professional standards.

Designated owners of records of archival value should arrange for Archives & Special Collections to review such records prior to disposal. Archives & Special Collections will assess the records for potential inclusion within the University Archive, in line with the Collections Development Policy – Archives & Special Collections. Archives & Special Collections will arrange for the transfer of any records selected for inclusion.

Transfers to the University Archive will typically occur at the point of disposal, after the end of any retention period. Where appropriate however, Archives & Special Collections may also accept records for inclusion within the University Archive during their retention period – this will typically be the case for records of archival value which have very long or indefinite retention periods.

In exceptional circumstances, Archives & Special Collections can provide storage for physical records with very long or indefinite retention periods, without incorporating them into the University Archive. Such records are not covered by the 'archiving purposes in the public interest' exemption of the Data Protection Act 2018, and remain the responsibility of their designated owner.

Further advice and guidance on any of these points can be obtained from Archives & Special Collections at archives@surrey.ac.uk.

Designated Owners

4.25. All systems and records must have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, University area, and level of access to the data required.

4.26. Data and records are never reviewed, removed, accessed, or destroyed without the prior authorisation and knowledge of the designated owners. These owners will also be responsible for continually reviewing the retention schedule for items that they own, ensuring accuracy by updating the schedule accordingly if any retention periods or details have changed.

Storage & Access of Records and Data

4.27. When stored, documents should be grouped together by category and in clear date order. Documents are always retained in a secure location, with access restricted to the authorised personnel.

4.28. Once the retention period has elapsed, the documents are either reviewed, archived, or confidentially destroyed depending on their purpose, classification, and action type.

Expiration of Retention Period

4.29. Once a record or data set has reached its designated retention period date, the designated owner should refer to their asset register for the action to be taken.

4.30. Not all data sets or records are expected to be deleted upon expiration; it may be sufficient to anonymise the data in accordance with data protection requirements or to archive records for a further period.

Suspension of Record Disposal for Litigation or Claims

4.31. If the University is served with any legal request for records or information, or any employee becomes the subject of an audit or investigation, or the University is notified of the commencement of any litigation against the University, the disposal of any scheduled records will be suspended until the University are able to determine the requirement for any such records as part of a legal requirement.

Paper Records

4.32. Where the University retains personal information in a paper format, it has a duty to ensure that these are stored securely. Once the retention period is met, they should be destroyed in a secure, confidential, and compliant manner, if not selected for archiving. The University utilises onsite shredding of all paper materials in Stag Hill House Records Store. Shredding machines and confidential waste sacks are made available to employees and where the University use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

Electronic Records and Systems

4.33. The University uses numerous systems, and technology equipment in the running of its business. From time to time, such devices must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

4.34. University data must not be retained on personal devices. Where university data is stored on a personal device it must be removed immediately as the security on the device is unlikely to meet

university standards.

Emails, Internal Correspondence, and General Memoranda

4.35. Unless otherwise stated in this procedure or the retention periods schedule, correspondence and internal memoranda should be retained for the same period as the document to which they support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed). This supporting material must be stored alongside the principal documents(s) in the appropriate University storage location and retained in an individual's files or email accounts.

4.36. Correspondence or memoranda that do not support any documents having already been assigned a retention period, should be deleted or shredded once the purpose and usefulness of the content ceases. Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General enquiries and replies
- Letter, notes or emails of inconsequential subject matter

4.37. Staff are reminded that emails are a transitory medium and that the University email system is not an additional storage space and should not be treated as such. Important material should be retained in a correctly managed file storage area that is not part of the email system.

Erasure

4.38. In specific circumstances, a data subject has the right to request that their personal data is erased. However, the University recognises that the 'right to be forgotten' is not absolute. The right to have personal data erased and to prevent processing only applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent (when the personal data is collected under this lawful basis.)
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- Where the data is not being processed under the 'archiving purposes in the public interest' exemption of the Data Protection Act 2018.
- The personal data was unlawfully processed.
- The personal data must be erased to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

4.39. Where the University receives a request to erase data the first step will be to determine which data sets the right of erasure applies to, if any. If the right does apply, the erasure will be carried out under instruction of the Information Governance department in conjunction with the relevant departments to ensure that all data relating to that individual has been erased. Erasure must take place within 30 days of the request being received.

4.40. Whilst standard procedures already remove data that is no longer necessary, a dedicated process

will be followed for erasure requests to ensure that all rights are complied with, and that no data has been retained for longer than is needed.

4.41. If for any reason, the University is unable to act in response to a request for erasure, a written explanation will be provided to the individual and inform them of their right to complain to the Supervisory Authority.

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
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- The Common Law Duty of Confidentiality
- Information Commissioners Office 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
- The National Archives Guide to archiving personal data 2018

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 has been completed on 07/10/2025 and is held by the Authorised Coordinator.

6.2. Procedure communicated to all subsidiaries on 13/11/2025.

6.3. Stakeholder consultation was completed as follows –

Stakeholder	Nature of Engagement	Request EB Approval (Y/N)	Date	Name of Contact
Governance	Consultation	N	08/10/2025	Kelley Padley
H&S	Consultation	N	24/10/2025	Matthew Purcell, Director of Health and Safety
Sustainability	Consultation	N	18/12/2025	Martin Wiles
Academic Freedom of Speech	Consultation	N	23/12/2025	Joshua Andresen
Director of Human Resources	Consultation	N	20/10/2025	Katy Huetson (Associate Director, People Services) on behalf of Sarah Leggett
Archives and Special Collections Manager	Consultation	N	14/10/2025	Helen Roberts