Policy

Documentation Retention and Secure Storage Policy

Document Title	Documentation Retention and Secure Storage Policy
Document Owner	IT Department
Approved By	Information Steering Committee
Date Approved	02 October 2023
Date of Review	10 December 2026
Document Version	1.2

Table of Contents

1. Purpose

This policy sets out the principles and requirements governing the retention, secure storage, and disposal of institutional documentation and records at London Campus of Higher Studies ("the Institution"), a higher education provider based in the United Kingdom. It is designed to ensure that records are kept for as long as they are needed to meet legal, regulatory, academic, and operational requirements, are held securely throughout their lifecycle, and are disposed of appropriately once no longer required.

This policy supports compliance with UK data protection legislation (including the UK GDPR and the Data Protection Act 2018), HMRC and statutory financial record-keeping requirements, and relevant sector regulatory expectations.

2. Scope

This policy applies to all records and documentation created, received, or held by the Institution in the course of its business, in any format, including:

- Physical (paper) records, including files, forms, and correspondence.
- Electronic records, including documents, spreadsheets, emails, databases, and system-generated records.
- Records held on institutional servers, cloud services, portable devices, and third-party or outsourced systems.
- Records relating to learners, staff, governance, finance, estates, and general business operations.

This policy applies to all staff, contractors, agents, and third parties who create, handle, or have access to institutional records on behalf of the Institution. It should be read alongside the Data Protection Policy, the Information Security Policy, the Freedom of Information Policy (where applicable), and the Safeguarding Policy.

3. Policy Statement

The Institution will maintain accurate and complete records for the periods set out in its Retention Schedule, will store those records securely and proportionately to their sensitivity, and will dispose of records confidentially and irreversibly once the applicable retention period has expired, unless a legal, contractual, or legitimate business reason requires continued retention.

Records will not be kept for longer than necessary, in line with the data minimisation and storage limitation principles of UK data protection law.

4. Principles of Retention

1. Necessity: records are retained only for as long as required to fulfil the purpose for which they were created, or as required by law, regulation, or contractual obligation.
2. Consistency: retention periods are applied consistently across the Institution in accordance with the approved Retention Schedule (see Section 6).
3. Accountability: the Institution can demonstrate, on request, why a given category of record is retained for its specified period.
4. Review: records approaching the end of their retention period are reviewed prior to disposal to confirm no further business, legal, or regulatory need exists.

5. Exceptions: retention periods may be extended where records are subject to a legal hold, ongoing investigation, complaint, litigation, or a Subject Access Request.

5. Secure Storage Requirements

5.1 Physical Records

Physical records containing personal, confidential, or commercially sensitive information must be stored in lockable cabinets, rooms, or archive facilities with access restricted to authorised personnel. Records must not be left unattended in public or unsecured areas, and visitor or shared spaces must not be used for document storage.

5.2 Electronic Records

Electronic records must be stored on institutional systems that are protected by appropriate access controls, authentication, encryption (where the record contains personal or sensitive data), and regular backup. Storage of institutional records on personal devices, personal cloud accounts, or unapproved third-party applications is not permitted.

5.3 Access Control

Access to records will be granted on a role-appropriate, least-privilege basis. Access to particularly sensitive records, such as safeguarding files or special category data, will be restricted to named individuals with a legitimate need to know.

5.4 Third-Party and Cloud Storage

Where records are held by a third-party processor or cloud service provider, the Institution will ensure that a data processing agreement is in place, that the provider meets the Institution's security standards, and that data is held within jurisdictions compliant with UK data protection requirements.

6. Retention Schedule (Summary)

The table below summarises indicative minimum retention periods for the principal categories of institutional record. The full Retention Schedule, maintained separately by the IT Department in consultation with the Data Protection Officer, takes precedence in the event of any discrepancy.

Record Category	Minimum Retention Period	Basis / Notes
Learner application and admissions records	6 years after last contact	Supports appeals, references, and regulatory audit.
Learner academic records (results, transcripts, awards)	Permanent (core record); supporting evidence 6 years	Core award record retained indefinitely for verification purposes.
Financial records (fees, invoices, payroll)	6 years plus current year	Aligned to HMRC and statutory audit requirements.
Staff employment records	6 years after employment ends	Longer where pension, litigation, or safeguarding matters apply.
Safeguarding and DBS-related records	As specified in the Safeguarding Policy	Subject to enhanced confidentiality controls.
Health and safety incident records	3–7 years depending on incident type	Longer for incidents involving minors or serious injury.

Governance records (minutes, policies)	10 years	Retained to evidence institutional decision-making.
General correspondence and working papers	2 years, unless superseded	Reviewed and disposed of once no longer of business value.

7. Secure Disposal

Records that have reached the end of their retention period, and for which no further business or legal need has been identified at review, will be disposed of securely:

- Physical records will be destroyed by cross-cut shredding or a certified confidential waste disposal contractor.
- Electronic records will be permanently deleted, including from backups where feasible within standard backup cycles, using secure deletion methods appropriate to the storage medium.
- Disposal of records containing personal or sensitive data will be logged, recording the record category, disposal date, and method.

Records subject to a legal hold, ongoing complaint, investigation, or litigation will not be disposed of until that matter has concluded, regardless of the standard retention period.

8. Data Breach and Incident Reporting

Any suspected loss, unauthorised access, or breach of security relating to institutional records, whether physical or electronic, must be reported to the IT Department and the Data Protection Officer immediately and in any event within 24 hours of discovery, in accordance with the Institution's Data Protection Policy and Incident Response Procedure.

9. Business Continuity and Backup

The IT Department will maintain a documented backup regime for electronic records held on institutional systems, with backups tested periodically to confirm records can be restored. Critical records will be included within the Institution's Business Continuity and Disaster Recovery Plan.

10. Monitoring, Compliance, and Review

Compliance with this policy will be monitored through periodic internal audit and spot-checks of physical and electronic storage areas. Breaches of this policy may be addressed through the Institution's disciplinary procedures where appropriate.

This policy is reviewed periodically to ensure it remains accurate, effective, and compliant with current legislation and sector requirements. This version was approved by the Information Steering Committee on 02 October 2023 and is scheduled for review on or before 10 December 2026, or sooner if required by a material change in legislation or institutional practice.

11. Related Policies and Documents

- Data Protection Policy
- Information Security Policy
- Retention Schedule (full version)
- Safeguarding Policy

- Freedom of Information Policy
- Business Continuity and Disaster Recovery Plan
- Incident Response Procedure

12. Roles and Responsibilities

Role	Responsibility
Information Steering Committee	Approves the policy and any substantive amendments; ensures alignment with institutional strategy, information governance, and legal obligations.
IT Department (Document Owner)	Maintains and publishes the policy, manages version control, coordinates the review cycle, and administers the technical and system-level controls that support secure storage.
Data Protection Officer	Advises on retention periods, data subject rights, and compliance with UK data protection legislation; approves the institutional Retention Schedule.
Academic Registry	Retains, archives, and disposes of learner records in accordance with the Retention Schedule.
Heads of Department	Ensure staff within their area understand and apply this policy to documents and records they create or hold.
All Staff	Store, handle, and dispose of institutional documentation in accordance with this policy and report any suspected loss or breach without delay.

Aamer Ali Aamer Ali	Muhammad Saqib Sohail Saqib Sohail
Director Admin / Operations	Director Academic Affairs
10 December 2025	10 December 2025