Inspire London College

Document Retention and Secure Storage Policy

Document Retention and Secure Storage Policy	Last Review:	September 2025
	Amended Date:	N/A
	Next planned review in 12 months, or sooner as required	

Document Retention and Secure Storage Policy

1. Introduction

Inspire London College is committed to maintaining high standards of data protection and document security. This policy establishes clear guidelines for the retention, secure storage, and disposal of records, ensuring that learner and institutional data are safeguarded against unauthorised access, loss, or misuse. It also ensures compliance with regulatory requirements and awarding body policies for document retention.

The College maintains different categories of records, including learner records, assessment submissions, certification records, financial documents, and administrative files. The retention period for each category varies depending on legal, academic, and operational requirements.

2. Scope

This policy applies to all learners, staff members, and stakeholders of Inspire London College. It outlines the procedures for the retention, storage, and secure disposal of documents in compliance with UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and awarding body regulations. The policy ensures that learner records, assessment documents, administrative records, and other sensitive information are managed securely and retained for the required period before being disposed of appropriately.

3. Categories of Documents and Retention Periods

The College classifies documents based on their purpose and sensitivity. The retention periods for key document categories are as follows:

3.1 Learner Records

All learner-related documents, including enrolment forms, identity verification documents, and academic records, are retained for a period of six years after the learner has completed or withdrawn from their course. This ensures that records remain available for verification requests and regulatory compliance.

3.2 Assessment and Examination Records

Assignment submissions, examination scripts, assessor feedback, and grading records are retained for a minimum of three years from the date of assessment. This aligns with the requirements of awarding bodies for quality assurance and external audits.

3.3 Certification Records

Records of issued certificates, including certificate numbers and dates of issuance, are maintained indefinitely to facilitate future verification requests by learners, employers, and external organisations.

3.4 Financial and Transactional Documents

Documents related to learner fee payments, invoices, and refunds are retained for a minimum of six years, in compliance with financial and tax regulations.

3.5 Staff and HR Records

Employment contracts, payroll records, and performance reviews are retained for six years after an employee leaves the College. Any records related to disciplinary actions are retained for six years, unless legal or regulatory requirements specify otherwise.

3.6 Policies, Procedures, and Institutional Documents

College policies, governance records, and internal meeting minutes are retained for a minimum of ten years, unless they are superseded by updated versions.

4. Secure Storage of Documents

All documents, whether physical or electronic, must be stored securely to prevent unauthorised access, loss, or tampering. The College implements the following measures for secure document storage:

4.1 Physical Document Storage

Hard copies of learner records, financial transactions, and assessment records are stored in locked filing cabinets or secure archive rooms. Access to physical documents is restricted to authorised personnel only. Sensitive documents are not left unattended in open areas, and all paper records containing personal data are handled in compliance with data protection regulations.

4.2 Electronic Document Storage

Digital records are stored on secure servers with restricted access. Encrypted cloud storage and password-protected databases are used to safeguard learner and institutional data. Access to electronic records is granted based on role-specific permissions, ensuring that only authorised staff can view, edit, or manage sensitive information.

4.3 Data Backup and Disaster Recovery

Regular backups are conducted to prevent data loss. All electronic records are backed up on a secure, encrypted server, with offsite backup facilities in place to ensure data recovery in case of system failure. Disaster recovery protocols are reviewed periodically to maintain data security and compliance.

5. Document Access and Retrieval

Only authorised personnel have access to specific categories of records. Requests for access to learner records, assessment submissions, or certification details must be submitted in writing and approved by the designated data protection officer. Learners can request copies of their records, in accordance with their rights under UK GDPR, by submitting a formal request to the College's administration team.

6. Secure Disposal of Documents

Once the retention period has expired, documents must be securely disposed of to prevent unauthorised access or misuse.

6.1 Disposal of Physical Documents

Paper records containing personal or confidential information are shredded and disposed of in compliance with data protection regulations. Shredding is conducted either in-house or through a certified document destruction service to ensure complete data elimination.

6.2 Disposal of Electronic Records

Digital records that are no longer required are permanently deleted from storage systems. Hard drives and other storage devices containing sensitive data are securely wiped or physically destroyed before disposal to prevent data recovery.

7. Breach Prevention and Incident Reporting

The College implements strict measures to prevent data breaches and unauthorised access to records. Any suspected breach of document security must be reported immediately to the Data Protection Officer (DPO). If a data breach occurs, an internal investigation will be conducted, and appropriate corrective actions will be taken. Where necessary, regulatory authorities and affected individuals will be informed in accordance with UK GDPR breach notification requirements.

8. Compliance and Monitoring

The College conducts regular audits to ensure compliance with this policy and relevant data protection laws. Any discrepancies in document handling or security procedures are addressed through staff training and policy updates.