Document & Data Retention Policy

Policy no:	6.02	**Version Number**	V2
Version Date	July 2025	**Next Review Date**	July 2026
Produced by	Director of Academy Advancement and Operations	**Approved by**	Senior Leadership Team
External reference points	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • Freedom of Information Act 2000 (FOIA) • Limitation Act 1980 • JISC Records Retention Schedule • Ofqual and Awarding Body Requirements (e.g. Pearson BTEC) • QAA (Quality Assurance Agency) Guidance • HESA (Higher Education Statistics Agency) • RIDDOR 2013 Regulation • Regulatory Reform (Fire Safety) Order 2005 • Control of Substances Hazardous to Health (COSHH) 2002 • Control of Asbestos Regulations 2012 • HM Revenue & Customs (HMRC) Requirements • Health and Safety at Work etc. Act 1974 • Control of Substances Hazardous to Health (COSHH) 2002 • Office of the Independent Adjudicator for Higher Education (OIAHE)		

Contents

1. Introduction

This policy outlines LCK Academy's approach to managing documents and records in both physical and electronic formats. It ensures that information is stored securely, retained for appropriate periods, and disposed of responsibly, in line with legal, regulatory, and operational requirements

2. Purpose

The purpose of this policy is to ensure that LCK Academy manages records and documents responsibly, in compliance with legal, regulatory, and awarding body requirements, and to support efficient academic and administrative operations.

3. Scope

This policy applies to all records created, received, or maintained by LCK Academy in both physical and electronic formats, including but not limited to:

- Student records
- Staff records
- Financial records
- Course and assessment documentation
- Communications and policies
- Health and Safety related activities

4. Aims and Objectives

The aims and objectives of this policy are to:

1. Ensure Legal Compliance
   Ensure that LCK Academy complies with all relevant legislation and regulatory requirements, including the UK GDPR, Data Protection Act 2018, and other sector specific guidelines.

2. Support Effective Record Management
   Promote consistent and responsible management of records across all departments to support operational efficiency, accountability, and good governance.

3. Protect Confidentiality and Integrity
   Safeguard sensitive and personal data by ensuring secure storage, access control, and timely disposal in line with data protection laws.
4. Facilitate Retention and Disposal

Provide a clear retention schedule to guide staff on how long different types of documents should be kept and when they should be securely disposed of.

5. Maintain Organisational Memory
   Preserve important institutional records that are necessary for historical reference, legal defence, quality assurance, or strategic planning.

6. Raise Awareness and Accountability
   Ensure that all staff understand their roles and responsibilities in managing records appropriately and report any breaches or concerns regarding data misuse or loss.

5. Staff Responsibilities

All LCK Academy staff share responsibility for managing records in line with this policy.

- **The Director of Advancement and Operations must:**
  - Oversee policy implementation and training.
  - Ensure that retention schedules are followed.
  - Approve and log secure disposal of documents.
  - Act as the lead point of contact for policy queries

- **Senior Leadership Team**
  - Monitor compliance with this policy in their teams.
  - Support training and good practice in document handling.
  - Approve and oversee secure document disposal.

- **All staff must:**
  - Be familiar with this policy and the retention schedule relevant to their role.
  - Store records securely and prevent unauthorised access.
  - Avoid retaining documents beyond their required period.
  - Report any concerns regarding data loss or misuse immediately.

- **Academic and administrative staff must:**
  - Maintain accurate records for students, courses, and assessments.
  - Dispose of obsolete documents, drafts, and duplicates responsibly.

6. Retention Schedule

Document Type	Retention Period	Source
Student admission records	1 year after admission cycle ends for unsuccessful applications	Administrative reference
Enrolled/registered student records (e.g. personal details, attendance, assessments, complaints)	6 + 1 years after student leaves	Limitation Act 1980, OfS
Student Contract Documents (e.g. Terms and Conditions, Offer Letters, Policies forming part of the contract)	Maximum period of the student's registration + 3 years	To comply with consumer protection law and CMA guidance.
Final awards and qualification data	OfS – Indefinitely Pearson – minimum 40 years	OfS and Pearson
Assessment and internal verification records	3 years after academic year ends	Pearson requirement
Complaints and appeals	6 years after resolution	Legal and regulatory compliance, (OIAHE)
Safeguarding records	6 years after last contact with student	Safeguarding policy
Staff HR files	6 years after employment ends	Employment legislation
Financial records (e.g. invoices, receipts)	6 years from end of financial year	HMRC requirement
Policies and procedures	Until superseded + 3 years	Governance and accountability
Emails and communications	2 years (unless related to a formal record)	Operational use
Accident/incident reports (general)	3 years from date of incident (for adults)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)
Accident records relating to children	Until the child reaches age 21 (i.e., 3 years after turning 18)	Limitation Act 1980
RIDDOR reports	3 years from date of report	RIDDOR 2013 Regulation 12
Risk assessments (general)	As long as they are relevant + recommended: 5 years minimum	Management of Health and Safety at Work Regulations 1999
Fire safety records (e.g. drills, inspections, training)	3 years	Regulatory Reform (Fire Safety) Order 2005

Health surveillance records (e.g., for hazardous substances)	40 years	Control of Substances Hazardous to Health (COSHH) 2002
Asbestos-related records	40 years from date of last entry	Control of Asbestos Regulations 2012
Records of first aid administered	3 years from date of incident	Health and Safety (First Aid) Regulations 1981
Academic Governance structure, board and committees' paperwork, including strategy documents and plans	Permanent or 10 years (if strategy-based)	Institutional memory, quality assurance
Annual monitoring reports	Current year + 6 years	Quality assurance and regulatory compliance
Student feedback and surveys	Current year + 6 years	Continuous improvement and monitoring
External examiner reports	Current year + 6 years	QA evidence and audit trail
Programme administration records (timetables, exam schedules, invigilation)	Current year + 6 years	QA, student complaints, regulatory evidence
Exam board minutes, results, and conferment lists	Permanent (summary records) / 10 years (detailed records)	Qualification verification, academic record
Audit records and internal audit reports	6 years (Companies Act), up to 10 if risk-based	Financial and legal compliance
Risk management registers, reports, and actions	6 years minimum (longer for key institutional risk)	Risk governance and legal defence
Marketing materials, website archives, communications	Current year + 3 years	Brand compliance and historical record
Project documents, reports, evaluations	Project closure + 6 years	Audit, evaluation, and institutional learning
Estate legal records (e.g. leases, site surveys, plans)	Duration of ownership/lease + 12 years	Limitation Act 1980; land/property evidence

General Student Support Records (e.g. learning plans, pastoral support)	6 years after the student leaves	Aligned with the Limitation Act 1980 and common practice in education for contractual or negligence claims.

7. Storage and Security

All records must be stored securely to protect confidentiality, integrity, and accessibility.

- Physical records should be kept in locked cabinets or secure storage areas.
- Electronic records must be backed up regularly, with access controls based on staff roles and responsibilities.
- Sensitive data must only be accessible to authorised personnel.

8. Disposal

When documents reach the end of their retention period, they must be disposed of securely:

- **Paper records**: must be shredded or professionally destroyed.
- **Digital records**: must be permanently deleted from all systems, servers, and backups.

A record of all document disposals must be kept, including the type of document, disposal date, and authorising personnel

9. Data Protection Compliance

LCK Academy complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

All personal data must be processed in accordance with the Academy's Data Protection Policy, ensuring lawfulness, fairness, transparency, and data minimisation.

10. Review and Oversight

This policy will be reviewed annually and updated as necessary to reflect legal or operational changes. The Director of Advancement and Operations is responsible for:

- Ensuring compliance with this policy.

- Coordinating annual reviews.
- Overseeing secure document disposal.
- Maintaining disposal logs.
- Providing training and guidance to staff on document management.