Data Retention Schedule

London Academy for Applied Technology (LAAT) – companion to the Record Management Policy (LAATITPOL009)

Document reference	LAATITPOL011 [confirm reference number]
Department / Function	IT (in partnership with the Data Protection Officer)
Owner	Head of IT / Data Protection Officer
Oversight committee	Audit & Risk Committee (Risk Assessment & IT Panel)
Approving body	Board of Governors
Version	v1.0
Status	Final – for approval
Date approved	Pending committee approval
Review date	Two years from approval (or sooner on regulatory change)
Parent policy	Record Management Policy (LAATITPOL009)

1. Purpose and relationship to the Record Management Policy

This Data Retention Schedule is the companion document to LAAT's Record Management Policy (LAATITPOL009). The policy sets out how records are created, classified, stored, retained and disposed of; this schedule specifies, for each category of record, how long it is kept and what happens at the end of that period. It is maintained separately so that retention periods can be updated without re-approving the full policy.

2. Scope

This schedule applies to all records created or received by LAAT in any format, across all campuses, remote-working environments and cloud-hosted services (including the Microsoft 365 environment), and to all staff, students, contractors and third parties who handle LAAT records.

3. How to use this schedule

- Identify the record category in the table below that best fits the record.
- Apply the stated retention period from the relevant trigger date.
- Where practicable, apply the period through system controls (for example Microsoft 365 retention labels).
- At the end of the period, the Record Owner authorises disposal in line with the Record Management Policy.

4. Retention schedule

The periods below are minimum retention periods. They are read alongside, and do not override, any longer period required by statute, by funding bodies (for example ESFA), by HMRC, or by LAAT's awarding partner, Plymouth Marjon University. Where more than one requirement applies, the longest period is used.

Record category	Examples	Retention period	Trigger / disposal action
Applicant records (unsuccessful / withdrawn)	Application forms, enquiries, supporting documents	1 year after the end of the admissions cycle	Securely delete after trigger

Student academic record (core)	Enrolment, programme, results, transcripts, certificates, awards	Core award record: permanent; full student file: 6 years after course completion / withdrawal	Archive core record; securely destroy wider file after 6 years
Student support & wellbeing	Support plans, reasonable adjustments, counselling notes	6 years after last contact (longer where there is ongoing risk)	Securely destroy after trigger
Fees & financial records	Invoices, payments, refunds, financial support	7 years (current financial year plus 6), per HMRC	Securely destroy after trigger
Apprenticeship records	Learner files, evidence packs, off-the-job logs, EPA records	Minimum 6 years after the end of the funding agreement, per ESFA funding rules	Retain for ESFA audit; destroy after period
Safeguarding & Prevent records	Concerns, referrals, DSL records	Retained securely; records relating to under-18s kept until the individual is 25, and longer for serious incidents or legal proceedings	Review before destruction
Complaints, appeals & conduct	Complaints, academic appeals, disciplinary cases	6 years after case closure	Securely destroy after trigger
Staff / HR records	Contracts, payroll, recruitment, training, conduct	6 years after employment ends (payroll/tax: 7 years)	Securely destroy after trigger
Governance records	Board & committee minutes, policies, registers of interest	Permanent (minutes & key decisions); superseded policies 6 years	Archive permanently
Health & safety records	Risk assessments, accident records	Accident records: 3 years from the date of entry; longer where required by RIDDOR / COSHH	Securely destroy after trigger
Marketing & consent	Newsletter sign-ups, consent records, enquiry forms	Until consent is withdrawn or after 24 months of inactivity	Delete on withdrawal / lapse
IT & system logs	Access logs, security logs, CCTV	Access/security logs: 6–12 months; CCTV: 30 days	Automatic overwrite / secure deletion

5. Disposal

At the end of the retention period, digital records are permanently deleted from systems and from backups in due course, and physical records are securely destroyed. Disposal is authorised by the relevant Record Owner and, for personal data, is consistent with the Data Protection Policy. Disposal activity is documented.

6. Legal holds

Where litigation, investigation or regulatory action is actual or anticipated, relevant records are placed on legal hold and preserved, overriding the periods in this schedule, until the hold is formally lifted.

7. Review

This schedule is reviewed by the Head of IT and Data Protection Officer at least every two years, or sooner if legislation, funding rules or awarding-body requirements change. Any change to a retention period is recorded in the version history.

8. Related documents

- Record Management Policy (LAATITPOL009)
- Data Protection Policy / GDPR
- Data Subject Access Request (DSAR) Policy (LAAT-IT-POL-002)
- Information Security Policy (LAATITPOL003)
- Privacy Notice (LAATITPOL010)