Record Management Policy

Document reference	LAATITPOL009
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	Draft
Date approved	22-06-2026
Review date	Annually from the approval date
Supersedes	N/A

1. Purpose

This policy establishes how London Academy for Applied Technology (LAAT) creates, classifies, stores, retains and disposes of its records, whether held in digital or physical form. Its purpose is to ensure that records are managed consistently and lawfully, are available when needed, are retained for no longer than necessary, and are disposed of securely. Effective record management supports operational efficiency, regulatory compliance, and LAAT's obligations to students, staff and partners.

2. Scope

- **Who:** All LAAT staff, students, contractors and third parties who create or handle LAAT records.
- **What:** All records created or received in the course of LAAT business, including student records, academic and assessment records, staff and HR records, governance and committee records, financial records, and IT and system logs, in any format (digital, email, paper or other media).
- **Where:** All LAAT campuses (Tower Hill, Brentford and Croydon), remote-working environments and cloud-hosted services, including the Microsoft 365 environment (SharePoint, Exchange Online, Teams) and connected systems.

This policy works alongside the Data Protection Policy, which governs the handling of personal data specifically; this policy addresses records management generally, including records that are not personal data.

3. Definitions

- **Record –** information created, received and maintained as evidence of LAAT's activities or because of legal or regulatory obligation, regardless of format.
- **Retention Schedule –** a document specifying how long each category of record is kept and the action taken at the end of that period.
- **Retention Period –** the length of time a record must be kept to satisfy operational, legal or regulatory requirements.

- **Disposal –** the secure destruction or transfer of a record once its retention period has expired.
- **Vital Record –** a record essential to LAAT's continued operation or to the protection of its or others' interests.
- **Legal Hold –** a requirement to preserve records relevant to actual or anticipated litigation, investigation or regulatory action, overriding normal disposal.

4. Principles

1. **Lawfulness and Compliance –** Records are managed in accordance with legal, regulatory and contractual requirements.
2. **Proportionate Retention –** Records are kept only as long as necessary and disposed of securely thereafter.
3. **Accuracy and Integrity –** Records are accurate, complete and protected against unauthorised alteration.
4. **Accessibility –** Records are organised so that they can be located and retrieved efficiently by authorised users.
5. **Security –** Records are protected against loss, damage and unauthorised access, in line with their sensitivity.
6. **Accountability –** Responsibility for records is clearly assigned and decisions are documented.

5. Governance, Committees and Terms of Reference

The Audit & Risk Committee, supported by the Risk Assessment & IT Panel (RITP), oversees this policy and receives reports on retention compliance, disposal activity and any record-related incidents. The Data Protection Officer advises on records that constitute personal data. The IT function maintains the systems in which records are stored and the technical retention controls.

6. Roles and Responsibilities

- **Policy Owner (Head of IT / Data Protection Officer) –** maintains and reviews this policy and the retention schedule, and oversees records management arrangements.
- **Information / Record Owners –** responsible for the records within their area, including classification, retention and authorised disposal.
- **IT Support Officers / Administrators –** implement technical retention and disposal controls (for example retention labels in Microsoft 365), maintain backups and apply legal holds when instructed.
- **Data Protection Officer –** advises on personal-data records, retention periods and lawful disposal.
- **All Staff and Students –** create and store records in approved locations, follow retention requirements, and do not dispose of records contrary to this policy.

7. Policy Statement

7.1 Record Creation and Classification

Records are created accurately and stored in approved institutional systems. Records are classified according to type and sensitivity so that appropriate handling, retention and security controls can be applied. Records must not be held solely in personal or unmanaged locations.

7.2 Storage and Security

Records are stored in secure, managed systems with access controlled in line with the Access Control Policy. Sensitive records receive enhanced protection. Vital records are identified and protected through backup and continuity arrangements.

7.3 Retention

Records are retained for the periods set out in LAAT's retention schedule, which reflects legal, regulatory, funding and partner requirements. Retention periods are applied through system controls, such as Microsoft 365 retention labels, wherever practicable.

7.4 Disposal

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

7.5 Legal Holds and Preservation

Where litigation, investigation or regulatory action is actual or anticipated, relevant records are placed on legal hold and preserved, overriding normal disposal, until the hold is lifted. LAAT uses appropriate tools (for example Microsoft Purview eDiscovery and retention/hold capabilities) to preserve records when required.

7.6 Transfer and Sharing

Records are transferred or shared only through secure means and only with authorised recipients. Sharing of personal data is governed by the Data Protection Policy.

7.7 Email and Collaboration Records

Email and collaboration content that constitutes a record is retained and managed according to the same principles as other records, and is subject to the retention schedule and any legal holds.

8. Standard Operating Procedure – Overview

Appendix A sets out the procedures for classifying records, applying the retention schedule, conducting secure disposal, applying legal holds, and handling record-related incidents.

9. Regulatory, Partner and Legal Alignment

This policy aligns with the UK GDPR and Data Protection Act 2018, the Freedom of Information Act 2000, the OfS conditions of registration (in particular Condition C and Condition C1 relating to information management), the requirements of the validating partner (Plymouth Marjon University), and funding and audit requirements. It will be updated in response to legislative, regulatory or contractual changes.

10. Monitoring, Compliance and Review

The Head of IT and Data Protection Officer monitor compliance through periodic reviews of retention and disposal. Non-compliance may result in corrective action and, where appropriate, disciplinary measures. The policy and retention schedule are reviewed every two years, or sooner following a significant change or incident.

11. Related Documents

- Data Protection Policy
- Data Subject Access Request (DSAR) Policy (LAAT-IT-POL-002)
- Information Security Policy (LAATITPOL003)
- Access Control Policy (LAATITPOL007)
- LAAT Retention Schedule
- Business Continuity Plan

Appendix A – SOP: Record Management

A1. Record Creation and Classification

1. Records are created in approved institutional systems and classified by type and sensitivity at the point of creation or receipt.
2. Records are not stored solely in personal or unmanaged locations.

A2. Applying the Retention Schedule

3. Each record category is mapped to a retention period in the LAAT retention schedule.
4. Retention is applied through system controls (for example Microsoft 365 retention labels) wherever practicable.

A3. Secure Disposal

5. At the end of the retention period, the Record Owner authorises disposal.
6. Digital records are permanently deleted from systems (and from backups in due course); physical records are securely destroyed.
7. Disposal of personal data follows the Data Protection Policy, and disposal activity is documented.

A4. Legal Holds

8. On notification of actual or anticipated litigation, investigation or regulatory action, IT applies a legal hold to the relevant records.
9. Held records are preserved and exempt from disposal until the hold is formally lifted.

A5. Record-Related Incidents

10. Loss, unauthorised disposal or unauthorised alteration of records is reported immediately to the Head of IT and, where personal data is involved, the Data Protection Officer.
11. The incident is investigated and remediated under the incident-response process.

A6. Review and Maintenance

12. This SOP and the retention schedule are reviewed every two years, following a major incident, or on significant regulatory change.