London Academy for Applied Technology

Information Security Policy

Document reference: LAAT-IT-POL-003
Department / Function: IT
Owner: Head of IT / Chief Information Security Officer
Oversight committee: Audit, Risk & Finance Committee
Approving body: Academic Board (recommendation) / Board of Governors (final approval)
Version: v1.0
Status: Adopted
Date approved: 18/02/2026
Review date: Annually from the approve date
Supersedes: None

Regularity Alignment with Office for Students conditions

This Information Security Policy forms part of the London Academy for Applied Technology's (LAAT) governance and information management framework and supports the secure, reliable, and resilient operation of institutional information systems and digital infrastructure.

The policy aligns with OfS Condition F2 (Information Controls) by establishing robust technical and organisational measures to protect personal and institutional data, ensure system integrity, and support accurate regulatory reporting.

It also supports Condition F1 (Provision of Information) by safeguarding the reliability and completeness of data used for statutory returns and public information. Furthermore, the policy aligns with Conditions E1, E2, and E3 (Public Interest Governance, Management and Governance, and Accountability) by embedding information security within institutional oversight arrangements, defining clear responsibilities, and providing assurance through monitoring, audit, and escalation processes.

The policy also supports Conditions B2 (Resources, Support and Student Engagement) and C5 (Treating Students Fairly) by ensuring that digital systems and learning resources are secure, accessible, and managed in a way that protects student interests and data rights.

Terms of Reference

1. Purpose

This policy provides a security framework that will ensure the protection of LAAT information from unauthorised access, loss or damage while supporting the open, information sharing needs of our academic community. the purpose is to protect institutional data across all media (verbal, digital and hardcopy), ensure operational continuity, minimise risk and allow LAAT to focus on its mission of teaching and research.

2. Scope

- **Who**: All LAAT staff, students, contractors, visitors and third-party service providers with access to LAAT information systems.
- **What**: All institutional data, information systems, networks, applications, devices, services and infrastructure, whether owned or leased, that are used to store or transmit LAAT information.
- **Where**: All LAAT campuses, data centres (server), cloud services and remote access environments.

This policy does not cover personal devices or accounts used exclusively for personal activities; however, any personal devices used for LAAT work must comply with BringYourOwnDevice (BYOD) guidelines set out in separate documentation.

3. Definitions

- **Information Asset** – any data or system that has value to LAAT, including research data, student records, financial data, intellectual property and infrastructure.
- **Confidentiality** – assurance that information is accessible only to authorised individuals.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that authorised users have access to information and associated assets when required.
- **Incident** – a breach or suspected breach of security that compromises confidentiality, integrity or availability of information.

4. Principles

1. **Confidentiality, Integrity and Availability (CIA)** – Information must be protected to preserve its confidentiality, integrity and availability.

2. **Risk Management** – Security measures will be proportional to the sensitivity of the information and the risk of compromise.

3. **Compliance** – LAAT will comply with all relevant laws, regulations and contracts governing information security.

4. **Continuous Improvement** – The security programme will be reviewed regularly to address emerging threats.

5. **User Awareness** – All users must be aware of their responsibilities and complete regular training.

5. Governance, Committees and Terms of Reference

Governance is provided by the Board of Governors. The Audit & Risk Committee oversees the Information Security Policy and receives reports on incidents and risks. An Information Security Working Group advises on implementation and ensures alignment with academic and operational needs.

6. Policy Statement

6.1 Information Classification and Handling

All information assets must be classified (e.g. public, internal, confidential, highly confidential) and handled according to their classification. Confidential and highly confidential data must be stored in secure systems and encrypted in transit and at rest.

6.2 Access Control

Access to systems and data will be granted on the principle of least privilege. Users must authenticate using secure credentials (e.g. multifactor authentication). User accounts must be reviewed regularly and revoked when no longer required.

6.3 Acceptable Use

Users must use LAAT information systems responsibly, refrain from unauthorised software installation, and comply with copyright and licensing requirements. Personal use of LAAT systems must be minimal and not compromise security.

6.4 Incident Management

All suspected or actual information security incidents must be reported immediately to the Information Security Officer. An incident response procedure will be followed, including containment, eradication, recovery and post incident review.

6.5 Physical Security

LAAT facilities must have appropriate physical controls (e.g. locked server rooms, visitor logs) to prevent unauthorised physical access to information systems.

6.6 Business Continuity and Disaster Recovery

Critical systems must have backup and recovery plans to ensure availability in case of disruptive events.

7. Standard Operating Procedure – Overview

Appendix A details processes for classifying information, granting access, managing passwords, handling incidents, patch management, and auditing.

8. Regulatory, Partner and Legal Alignment

This policy aligns with the UK GDPR, Data Protection Act 2018, OfS conditions (especially C1 and E2), validating university policies and any contractual obligations. It will be updated in response to legislative or regulatory changes.

9. Monitoring, Compliance and Review

The Information Security Officer will conduct regular risk assessments, audits and penetration tests. Noncompliance may result in disciplinary action or termination of access. The policy will be reviewed every two years or as required.

10. Responsible people/ roles includes

- **Head of IT / CISO (policy owner): Himanshu Chadha**
  maintains and reviews the policy, oversees security strategy and reports to the Audit & Risk Committee.
- **System Owners / Administrators**: **Bijay Shresta**
  classify and secure information assets within their remit, enforce access controls, maintain logs and ensure backups.
- **All Users** – adhere to security procedures, use strong passwords, report incidents or suspicious activities, and complete training.
- **Third-party Providers** – comply with contractually agreed security requirements and report incidents promptly.

List of people and contact

Role	**Name**	**Contact email**
Head of IT	Himanshu Chadha	himanshu@laat.ac.uk
Administrator	Bijay Shresta	bijay@laat.ac.uk
Data Protection Officer	Nadia Asim	nadiaasim@laat.ac.uk

11. List of Documents

- Data Protection Policy
- Data Subject Access Request (DSAR) policy
- Acceptable Use Policy
- Incident Response Plan
- BringYourOwnDevice (BYOD) Guidelines

12. Evidence

- Data Protection Policy
- Data Subject Access Request (DSAR) policy
- Incident Response Plan
- BringYourOwnDevice (BYOD) Guidelines

Evidence items mapping table

Evidence Item	**Purpose / What it Demonstrates**	**Relevant OfS Condition(s)**
Data Protection Policy	Establishes the institutional framework for lawful, secure, and transparent handling of personal data	F1 (information provision), F2 (information controls), E2 (management and governance)
Data Subject Access Request (DSAR) Policy	Provides formal procedures for handling subject access requests fairly and within statutory timescales	C1 (consumer protection), C5 (fair treatment), E2 (management and governance), E3 (accountability)
Incident Response Plan	Establishes structured procedures for managing data and cyber security incidents and breaches	F2 (information controls), E3 (accountability), E2 (management and governance)
Bring Your Own Device (BYOD) Guidelines	Provides controls for secure use of personal devices accessing institutional systems	F2 (information controls), E2 (management and governance), B2 (resources and support)

Appendix A – SOP: Information Security

The SOP provides procedures for information classification, user provisioning/deprovisioning, password management, incident handling, vulnerability management, encryption standards and physical security protocols. Templates and forms are available on the LAAT intranet (IT section).

SOP – Appendix A

A1. Purpose

This Standard Operating Procedure (SOP) defines the requirements for the creation, use, protection, and management of passwords used to access LAAT information systems. Its purpose is to reduce the risk of unauthorised access, data breaches, and system compromise by enforcing consistent and secure password practices.

A2. Scope

This SOP applies to:

- All LAAT staff, students, contractors, and third-party users
- All LAAT-managed systems, applications, networks, and cloud services
- All accounts with access to LAAT information assets, including administrative and privileged accounts

A3. Responsibilities

Information Security Officer (ISO)

- Defines password standards and authentication requirements
- Monitors compliance and investigates password-related security incidents

System Owners / Administrators

- Implement and enforce password controls on systems under their responsibility
- Ensure technical controls prevent weak or reused passwords

All Users

- Create and maintain secure passwords
- Protect their authentication credentials
- Report suspected credential compromise immediately

A4. Password Standards

All passwords must meet the following minimum requirements unless stronger controls are enforced by the system:

- Minimum length: **12 characters**
- Must include at least **three** of the following:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special characters

- Must not include:
    - Usernames, personal details, or easily guessable information
    - Previously used passwords (password reuse is prohibited)

Passwords must be system-enforced where technically possible.

A5. Multi-Factor Authentication (MFA)

- MFA is mandatory for:
    - Remote access
    - Cloud services
    - Privileged or administrative accounts
- Approved MFA methods include authenticator applications, hardware tokens, or other IT-approved mechanisms.
- SMS-based MFA should only be used where stronger options are not available.

A6. Password Storage and Transmission

- Passwords must never be stored in plain text.
- Systems must store passwords using approved cryptographic hashing algorithms.
- Passwords must not be shared, emailed, written down, or stored in unsecured locations.
- Approved password managers may be used where authorised by IT.

A7. Password Changes and Expiry

- Passwords must be changed:
    - Immediately if compromise is suspected
    - After a security incident involving credentials
- Routine password expiry will be enforced based on system risk:
    - High-risk or privileged accounts: **every 90 days**
    - Standard user accounts: **risk-based or event-driven**
- Forced periodic changes are avoided where MFA and strong passwords are in place, in line with best practice.

A8. Privileged and Service Accounts

- Privileged accounts must:
    - Use unique, strong passwords
    - Be restricted to named individuals
    - Be monitored and logged
- Service account passwords must:
    - Be stored securely
    - Be changed regularly or managed through automated credential vaults
    - Never be shared outside authorised administrators

A9. Lost or Compromised Credentials

- Users must report suspected or actual credential compromise **immediately** to the IT Service Desk or Information Security Officer.
- Compromised accounts will be:
  - Disabled or locked
  - Investigated under the Incident Response Procedure
  - Restored only after credentials are securely reset

A10. Monitoring and Compliance

- IT will monitor authentication logs for suspicious activity.
- Non-compliance with this SOP may result in:
  - Account suspension
  - Disciplinary action
  - Termination of access for third-party users

A11. Review and Maintenance

This SOP will be reviewed:

- Every two years
- Following a major security incident
- When significant changes to technology or regulatory requirements occur