London Academy for Applied Technology

IT Equipment and Acceptable Use Policy

Document reference: LAAT-IT-POL-006

Department / Function: IT

Owner: IT & Security Lead

Oversight committee: Risk Assessment & IT Monthly Panel (RITP); Audit, Risk & Finance Committee

Approving body: Academic Board (recommendation) / Board of Governors (final approval)

Version: v1.0

Status: Draft for Review

Date approved: TBC

Review date: Annually from the approve date

Supersedes: None

Regulatory Alignment with Office for Students conditions

This IT Equipment and Acceptable Use Policy forms part of the London Academy for Applied Technology's (LAAT) IT governance and information management framework. It supports the controlled, accountable, and resilient use of LAAT IT equipment, services and data by all staff, students, contractors, and visitors. It operates beneath the LAAT Information Security Policy (LAAT-IT-POL-003) and gives operational effect to its principles in the day-to-day management of devices, accounts, and IT service delivery.

The policy aligns with OfS Condition F2 (Information Controls) by establishing technical and operational measures over the equipment and accounts through which LAAT processes institutional and personal data, including controls for device allocation, recovery, replacement, and decommissioning.

It supports Condition F1 (Provision of Information) by safeguarding the reliability, integrity, and completeness of LAAT data held on or accessed through LAAT-issued equipment, on which statutory returns, the Register entry, and public information depend.

The policy aligns with Conditions E1, E2 and E3 (Public Interest Governance, Management and Governance, and Accountability) by defining clear responsibilities, authorisation routes, and escalation paths for IT equipment use and servicing; by embedding IT discipline within institutional oversight (RITP and SMT); and by establishing a documented, auditable basis for the actions of IT staff.

The policy supports Conditions B1 (Academic Experience), B2 (Resources, Support and Student Engagement), B3 (Student Outcomes), and B4 (Assessment and Awards) by ensuring that the IT equipment, services and data which underpin teaching, learning, assessment, and the student record are operated reliably and recoverable in the event of fault, loss, or misuse.

The policy supports Condition C1 (Consumer Protection guidance), Condition C2 (cooperation with the Office of the Independent Adjudicator student complaints scheme), and Condition C3 (Student

Protection Plan), and, where applicable, the new initial Condition C5 (Treating Students Fairly), by maintaining accurate, available, and recoverable student data and ensuring continuity of the IT services on which fair and timely communication with students depends.

The policy supports Condition D (Financial Sustainability) by establishing controls over the issue, return, repair, replacement, and accountability of LAAT-owned IT equipment as institutional assets, and contributes to compliance with Condition E4 (notification of changes to the OfS Register) and Conditions G2 and G3 (Accountability for fees and funding) by ensuring the data systems underlying registered information and financial reporting are operated under controlled and auditable conditions.

The policy is operated in conjunction with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Human Rights Act 1998 (in particular Article 8), the Protection from Harassment Act 1997, and applicable validating-partner requirements set by Plymouth Marjon University.

Terms of Reference

1. Purpose

This policy sets out the rules governing the use, handling, and servicing of IT equipment and digital services provided by LAAT. It defines the responsibilities of users and IT staff, the ownership of equipment and data, the authorised process for device collection, recovery, and replacement, and the standards of conduct expected of all parties when IT services are being delivered.

The policy exists to protect institutional data, ensure operational continuity of academic and administrative systems, maintain a professional and respectful working environment for IT staff, and provide a clear, auditable basis for IT service actions.

2. Scope

- **Who:** All LAAT staff, students, contractors, visitors, and third-party service providers with access to LAAT IT equipment, accounts, or services.
- **What:** All LAAT-owned or LAAT-leased IT equipment, software, accounts, credentials, and data created, received, stored, or processed through LAAT-licensed services (including Microsoft 365, Outlook, Teams, OneDrive, SharePoint, Moodle, and any other LAAT-procured application), whether accessed on-site, remotely, or on a personal device.
- **Where:** All LAAT campuses (Tower Hill, Brentford and Croydon), cloud services, and remote-access environments used to access LAAT services.

This policy does not cover personal devices used exclusively for personal activities. Use of personal devices for LAAT work is governed by the Bring Your Own Device (BYOD) Guidelines and remains subject to this policy in respect of any LAAT data, accounts, or credentials accessed on those devices.

3. Definitions

- **LAAT IT Equipment** — any hardware owned, leased, or otherwise provided by LAAT, including laptops, desktops, peripherals, mobile devices, removable media, and storage.
- **LAAT Data** — any data created, received, stored, or processed through LAAT credentials or LAAT-licensed services, regardless of the device on which the work is performed.

- **IT Service Action** — any action carried out by the IT team in the course of service delivery, including troubleshooting, configuration changes, data recovery, backup, factory reset, device collection, device replacement, and decommissioning.
- **Authorised Approver** — the user's line manager, the IT & Security Lead, the Operations Lead, or a member of the Senior Management Team.
- **Incident** — any event that compromises, or may compromise, the confidentiality, integrity, or availability of LAAT data, equipment, or services, including loss, theft, damage, unauthorised access, unauthorised recording, or deliberate deletion of LAAT data.

4. Principles

- **Institutional ownership:** LAAT IT equipment and LAAT data remain the property of LAAT at all times.
- **Proportionality and least privilege:** Access, controls, and IT service actions are proportionate to risk and operational need.
- **Authorisation and accountability:** All IT service actions are authorised, logged, and auditable.
- **Respect and cooperation:** Users and IT staff treat one another professionally; IT service delivery is supported, not obstructed, by users.
- **Compliance:** LAAT operates in line with UK law, OfS conditions, validating-partner requirements, and contractual obligations.
- **Continuous improvement:** Procedures are reviewed and updated based on incidents, audit, and emerging risks.

5. Governance, Committees and Terms of Reference

Governance is provided by the Board of Governors. The Audit, Risk & Finance Committee receives reports on IT incidents, asset risks, and policy compliance through the Senior Management Team. The Risk Assessment & IT Monthly Panel (RITP) provides operational oversight of IT risks, including those arising from equipment use and IT service delivery, and reviews material incidents and breaches arising under this policy. The IT & Security Lead is the policy owner and is responsible for day-to-day operation, monitoring, and review.

6. Policy Statement

6.1 Equipment Ownership and Issue

6.1.1 All IT equipment issued by LAAT remains the sole property of LAAT at all times. Possession of equipment by a user does not transfer ownership, and users acquire no rights over the device, its components, or its contents.

6.1.2 Devices are allocated by IT against a documented asset record. Users are responsible for the equipment in their possession, including its physical security, condition, and timely return on request or on separation from LAAT.

6.1.3 Users must not modify, transfer, lend, sell, or dispose of LAAT IT equipment. Reasonable wear and tear is accepted; damage, loss, or theft must be reported to itsupport@laat.ac.uk without delay.

6.2 Acceptable Use of IT Equipment and Services

6.2.1 Users must use LAAT IT equipment and services for legitimate work or study purposes. Personal use must be minimal, must not compromise security, and must not breach LAAT policy or UK law.

6.2.2 Users must:

- Keep devices physically secure and not leave them unattended in unsecured locations, including on desks, in public areas, or in unlocked vehicles;
- Comply with multi-factor authentication, device-compliance, and Conditional Access controls deployed via Microsoft Intune and related services;
- Not share login credentials, tokens, MFA codes, or password manager vaults;
- Use only software approved by IT, and refrain from installing unlicensed, pirated, or unverified software;
- Comply with copyright and licensing requirements at all times;
- Report faults, suspected security incidents, lost or stolen devices, and damage to itsupport@laat.ac.uk without delay;
- Cooperate fully and professionally with IT staff during any IT service action.

6.2.3 Users must not:

- Attempt to bypass security controls, including endpoint protection, device-compliance posture, or Conditional Access policies;
- Use LAAT credentials, equipment or accounts for purposes that breach LAAT policy or UK law;
- Connect unapproved removable media to LAAT devices;
- Delete, conceal, or remove LAAT data with the intent to prevent its recovery, audit, or disclosure under a legitimate institutional request.

6.3 Data Ownership and Handling

6.3.1 All LAAT data is the sole property of LAAT, regardless of whether the work was performed on-site, remotely, in or outside working hours, on a LAAT device, or on a personal device on which LAAT credentials were used.

6.3.2 Users have no right to retain, copy, transfer, or delete LAAT data without prior written authorisation from the data owner and the IT & Security Lead. Deliberate or negligent deletion of LAAT data may constitute a disciplinary offence and, where appropriate, a personal data breach reportable under the UK GDPR and the Data Protection Act 2018.

6.3.3 Users must store LAAT work in approved LAAT cloud locations (Microsoft 365 / OneDrive / SharePoint / Teams). Locally-stored data not synchronised to LAAT cloud services may not be recoverable in the event of a device fault, factory reset, or replacement.

6.3.4 IT may access, recover, restore, audit, or place legal hold on LAAT data on LAAT equipment and accounts for legitimate operational, security, compliance, eDiscovery, or investigatory purposes, in accordance with the LAAT Information Security Policy and Data Protection Policy.

6.4 Device Issues, Collection, Recovery and Replacement

6.4.1 Where a LAAT device develops a fault, the user must report it to IT via itsupport@laat.ac.uk or to their line manager. IT will attempt to resolve the issue in place where possible.

6.4.2 Where in-place resolution is not possible, IT may collect the device for service, including for factory reset, hardware diagnosis, data restoration, or replacement. Collection may be authorised by the user, the user's line manager (where the user is unavailable and the device is preventing work continuity), or the IT & Security Lead / Operations Lead on operational, security, or compliance grounds.

6.4.3 During an IT service action, the device is treated as out of service. Users are not entitled to interrupt, override, or remove the device from IT while the action is in progress, and are expected to remain reasonably available so that IT can provide updates and confirm completion.

6.4.4 Factory reset is a standard recovery step where in-place fixes fail. Microsoft 365 account data is generally recoverable from cloud retention points; IT will restore data to the most recent viable recovery point. Locally-stored data not synchronised to LAAT cloud services may not be recoverable (see 6.3.3).

6.4.5 Where IT determines that a device requires replacement on hardware, reliability, or security grounds, that decision is taken by the IT & Security Lead. The fact that a device is functioning at the end of a recovery process does not, by itself, override a replacement decision based on underlying hardware diagnosis, repeated faults, warranty status, or compliance posture.

6.4.6 Replacement devices are issued as soon as practicable. The user is responsible for signing for the device and verifying that data and access have been restored. Returned devices are securely wiped and decommissioned in line with the Information Security Policy.

6.5 Photography, Recording and Filming in IT Service Areas

6.5.1 Photography, video recording, audio recording, screen capture, or any other form of recording of IT staff, IT workstations, IT equipment, screens, or service activity, without the prior express consent of the IT & Security Lead (or, where appropriate, the individual member of IT staff being recorded), is prohibited.

6.5.2 This prohibition applies regardless of the device used (LAAT or personal), regardless of whether the image is shared, and regardless of the user's stated purpose. Stated explanations such as “for my safety” or “for my records” do not, on their own, constitute valid grounds for recording IT staff or service activity.

6.5.3 Any recording made in breach of 6.5.1 must be deleted immediately, including from the device's deleted-items or recycle bin and from any cloud backup. Confirmation of deletion must be provided in writing to the IT & Security Lead.

6.5.4 Recording captured during an IT service action may constitute the processing of personal data of IT staff and equipment-state information of LAAT, and may engage the UK GDPR, the Data Protection Act 2018, and Article 8 of the Human Rights Act 1998. A repeated pattern of such conduct may engage the Protection from Harassment Act 1997. Breach may be reported to the Information Commissioner's Office and may form the basis of disciplinary action.

6.5.5 Legitimate concerns about IT staff conduct must be raised in writing with the IT & Security Lead, the Operations Lead, or HR. Covert recording is not an appropriate substitute for this process.

6.5.6 Where IT staff need to capture screen content or device state for legitimate diagnostic, evidential, or audit purposes, this is permitted and is logged on the relevant IT ticket. Such captures are LAAT data and are handled under section 6.3.

6.6 Incident Reporting and Escalation

6.6.1 Users must report any IT issue, security concern, suspected data breach, or perceived breach of this policy to itsupport@laat.ac.uk in the first instance. Suspected personal data breaches are escalated to the Data Protection Officer without delay.

6.6.2 Concerns about the conduct of IT staff are raised in writing with the IT & Security Lead and may be escalated to the Operations Lead. Concerns about a user's conduct that affect IT service delivery are escalated by IT to the user's line manager, the Operations Lead, and HR as appropriate.

6.6.3 Material incidents are recorded on the IT incident register and reported through the RITP and SMT, with onward reporting to the Audit, Risk & Finance Committee and the Board of Governors where required.

6.7 Sanctions and Disciplinary Action

6.7.1 Breach of this policy may result in:

- Withdrawal or suspension of IT access;
- Disciplinary action under LAAT's Disciplinary Procedure, up to and including dismissal;
- Referral to law enforcement or the Information Commissioner's Office where the conduct may constitute a criminal offence or a personal data breach;
- Recovery of costs associated with damaged or unreturned equipment.

6.7.2 Particular conduct treated as serious breach includes: deliberate deletion or concealment of LAAT data; unauthorised recording of IT staff or service activity; obstruction of an IT service action; misuse of LAAT credentials; bypass of security controls; and unauthorised disclosure of LAAT data to third parties.

7. Standard Operating Procedure – Overview

Appendix A details the operating procedures supporting this policy, including device issue and allocation, acceptable use enforcement, device collection and IT service actions, data recovery and replacement, handling of photography and recording, and management of lost, stolen, or damaged devices. Templates and forms are available on the LAAT intranet (IT section).

8. Regulatory, Partner and Legal Alignment

This policy aligns with the UK GDPR, the Data Protection Act 2018, the Human Rights Act 1998, the Protection from Harassment Act 1997, the Computer Misuse Act 1990, the Office for Students conditions of registration (in particular F1, F2, E1, E2, E3, B2, C1, C3, and the new initial Conditions C5, E7, E8 and E9 in force from 28 August 2025), Plymouth Marjon University validating-partner requirements, and any applicable contractual obligations with third-party service providers. The policy will be updated in response to legislative or regulatory changes.

9. Monitoring, Compliance and Review

9.1 The IT & Security Lead monitors compliance through IT service records, asset audits, device-compliance reporting (Microsoft Intune), endpoint security telemetry (Microsoft Defender for Endpoint), and periodic review of authentication and audit logs.

9.2 Compliance with this policy is reviewed monthly at the Risk Assessment & IT Monthly Panel (RITP) and reported, with material findings, through the SMT to the Audit, Risk & Finance Committee.

9.3 Non-compliance may result in disciplinary action under section 6.7. Persistent or wilful non-compliance is reported through RITP and SMT for escalation.

9.4 This policy is reviewed annually, and additionally following any material incident, regulatory change, or significant change to LAAT's IT environment.

10. Responsible people / roles

- **IT & Security Lead (Policy Owner)** — maintains and reviews the policy; authorises IT service actions; chairs the RITP; reports to the Operations Lead and SMT.
- **IT Support Officer / IT Technicians** — deliver IT services; perform device collection, recovery, and replacement under documented authorisation; maintain ticket and asset records.
- **Data Protection Officer** — advises on personal data processing on LAAT equipment; receives and triages suspected personal data breaches.
- **Line Managers** — authorise device collection where the user is unavailable; support compliance with this policy within their teams; participate in disciplinary processes where required.
- **All Users** — comply with this policy; report incidents; cooperate with IT service actions; complete IT and information security training.
- **Third-party Providers** — comply with contractually agreed security and acceptable use requirements; report incidents promptly.

List of people and contact:

Role	Name	Contact email
IT & Security Lead (Policy Owner)	Himanshu	himanshu@laat.ac.uk
IT Support Officer (Administrator)	Bijay Shrestha	bijay@laat.ac.uk
IT Technician	Adrian Casapu	itsupport@laat.ac.uk
IT Technician	Adrian Bulgaru	itsupport@laat.ac.uk
Data Protection Officer	TBC	DPO@laat.ac.uk
IT Service Desk (shared mailbox)	—	itsupport@laat.ac.uk

11. List of Documents

- Information Security Policy (LAAT-IT-POL-003)
- Data Protection Policy

- Data Subject Access Request (DSAR) Policy
- Incident Response Plan
- Bring Your Own Device (BYOD) Guidelines
- Disciplinary Procedure (HR)
- Student Protection Plan
- Asset Register and IT Service Logs

12. Evidence

- Information Security Policy (LAAT-IT-POL-003)
- Data Protection Policy
- Bring Your Own Device (BYOD) Guidelines
- Incident Response Plan
- Asset Register and IT Service Logs
- Disciplinary Procedure (HR)
- Student Protection Plan

Evidence items mapping table:

Evidence Item	Purpose / What it Demonstrates	Relevant OfS Condition(s)
Information Security Policy (LAAT-IT-POL-003)	Parent framework for confidentiality, integrity and availability of LAAT information; provides the security baseline against which this policy is operated	F1 (provision of information), F2 (information controls), E1 (public interest governance), E2 (management and governance)
Data Protection Policy	Lawful, secure and transparent handling of personal data captured, stored or processed on LAAT IT equipment	F1, F2, E2, E3 (accountability)
Bring Your Own Device (BYOD) Guidelines	Controls for secure use of personal devices accessing LAAT systems and credentials	F2, E2, B2 (resources and support)
Incident Response Plan	Structured procedures for IT, data and security incidents arising from misuse, loss, damage or compromise of LAAT equipment	F2, E2, E3
Asset Register and IT Service Logs	Auditable record of LAAT IT assets, allocations, faults, IT service actions, recoveries and replacements	D (financial sustainability), E2, E3

Evidence Item	Purpose / What it Demonstrates	Relevant OfS Condition(s)
Disciplinary Procedure (HR)	Enforcement route for breaches of acceptable use, including obstruction of IT service actions and unauthorised recording of IT staff or equipment	E1, E2, E3, C1 (consumer protection)
Student Protection Plan	Continuity of IT services and student data underpins the institution's ability to deliver the protected outcomes for students	C3 (student protection plan), B2, B3 (student outcomes)

Appendix A – SOP: IT Equipment and Acceptable Use

A1. Purpose

This Standard Operating Procedure (SOP) sets out the operational steps that give effect to the IT Equipment and Acceptable Use Policy. It defines how devices are issued, used, serviced, recovered, replaced, and decommissioned, and how breaches of acceptable use are identified and managed.

A2. Scope

This SOP applies to:

- All LAAT staff, students, contractors, and third-party users with access to LAAT IT equipment or services;
- All LAAT-managed devices, accounts, applications, networks, and cloud services;
- All IT service actions performed by the LAAT IT team.

A3. Responsibilities

IT & Security Lead — authorises IT service actions; approves device collection, recovery, and replacement decisions; signs off on policy breach reports.

IT Support Officer / IT Technicians — carry out IT service actions; log all activity on the IT ticketing system; maintain asset records.

All Users — follow acceptable use standards; report faults and incidents; cooperate with IT service actions.

A4. Device Issue and Allocation

A4.1 IT issues devices against a documented asset record, recording device make and model, serial number, asset tag, allocated user, issue date, and accepted condition.

A4.2 The user signs an IT Equipment Issue receipt confirming acceptance of the device and acknowledgement of this policy and the LAAT Information Security Policy.

A4.3 Devices are pre-enrolled in Microsoft Intune and meet baseline compliance requirements (encryption, MFA, endpoint protection, OS update posture) before issue.

A5. Acceptable Use Standards

A5.1 Users comply with section 6.2 of the policy. Standard expectations include securing devices when unattended, refraining from sharing credentials, not installing unapproved software, and complying with applicable copyright and licensing requirements.

A5.2 IT monitors device-compliance posture through Microsoft Intune and Microsoft Defender for Endpoint. Non-compliant devices may have access restricted under Conditional Access until compliance is restored.

A6. Device Issues, Collection and IT Service Actions

A6.1 A device fault is reported by the user to itsupport@laat.ac.uk or to the user's line manager. A ticket is opened in the IT ticketing system.

A6.2 IT attempts in-place resolution where possible. Where the issue cannot be resolved in place, IT proposes a service action (e.g. factory reset, hardware diagnosis, replacement). The proposed action and its authorisation are logged on the ticket.

A6.3 Device collection may be authorised by the user, the user's line manager (where the user is unavailable and the device is preventing work continuity), or the IT & Security Lead or Operations Lead on operational, security, or compliance grounds. The authorisation is recorded on the ticket.

A6.4 During the service action, the device is treated as out of service. The user is not entitled to interrupt the action or remove the device from IT while the work is in progress. IT keeps the user reasonably informed of progress.

A6.5 Completion of the service action is confirmed in writing via the ticket or email, with the recovery point used and the data restoration status documented.

A7. Data Recovery and Replacement Procedures

A7.1 Recovery from Microsoft 365 cloud retention points is the standard data restoration method. Where multiple recovery points are available, IT selects the most recent viable point that restores user access without re-introducing the underlying fault.

A7.2 Locally-stored data not synchronised to LAAT cloud services may not be recoverable; users are reminded at issue and at every interaction that work files must be stored in approved cloud locations.

A7.3 Replacement decisions are taken by the IT & Security Lead on hardware, reliability, or security grounds. A device functioning at the end of recovery does not, by itself, override a replacement decision (see policy 6.4.5).

A7.4 Replacement devices are issued in line with A4, and the original device is securely wiped (in accordance with the Information Security Policy) and decommissioned.

A8. Photography, Recording and Filming

A8.1 Photography, video, audio, or screen recording of IT staff, IT workstations, IT equipment, or service activity without prior express consent of the IT & Security Lead is prohibited (policy 6.5.1).

A8.2 Where a recording is observed or suspected, the IT staff member politely informs the individual that recording is not permitted and asks them to stop and delete the recording, including from the device's deleted items and any cloud backup.

A8.3 The incident is logged on the IT ticketing system with: date, time, location, individuals involved, witnesses, what was recorded, the request to delete, and the user's response.

A8.4 The IT & Security Lead is notified the same day. Where appropriate, the matter is escalated to the Operations Lead, HR, and the Data Protection Officer.

A8.5 Where the recording captured personal data of IT staff or equipment-state information that may engage the UK GDPR, the matter is assessed by the DPO as a potential personal data breach.

A8.6 Repeated incidents involving the same individual are treated as a course of conduct and escalated for formal disciplinary action.

A9. Lost, Stolen or Damaged Devices

A9.1 Lost or stolen devices are reported to itsupport@laat.ac.uk and to the user's line manager without delay. Where the device may contain or access personal data, the DPO is notified the same day.

A9.2 IT remotely wipes the device through Microsoft Intune, revokes credentials, and disables MFA tokens registered to the device. The asset record is updated.

A9.3 For theft, the user reports the matter to the police and obtains a crime reference number, which is recorded on the IT ticket.

A9.4 Damaged devices are returned to IT for assessment. The cost of repair or replacement may be recovered from the user where damage results from negligence or breach of this policy.

A10. Monitoring and Compliance

A10.1 IT monitors authentication logs, device-compliance posture, endpoint telemetry, and IT ticketing data for indicators of misuse or non-compliance.

A10.2 Non-compliance may result in account suspension, restricted access, disciplinary action, or termination of access for third-party users (see policy 6.7).

A10.3 Material findings are reported through the RITP and SMT.

A11. Review and Maintenance

This SOP is reviewed annually, following any material incident, and when significant changes occur to LAAT's IT environment, technology stack, or applicable regulation. Reviews are owned by the IT & Security Lead and reported through the RITP.

Approval

Approved on behalf of London Academy for Applied Technology:

Name: _____

Role: _____

Signature: _____

Date: _____