London Academy for Applied Technology (LAAT)

Data Protection Policy

Policy title: Data Protection Policy
Document reference: LAAT-STD-POL-DP01
Department / Function: Governance, Compliance & Information Management
Policy Owner: IT, Mr Himanshu Chadha
Oversight Committee: Academic Board / 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 approval date
Supersedes: None

Regulatory Alignment with Office for Students (OfS) Conditions

This Data Protection Policy forms part of the London Academy for Applied Technology's (LAAT) governance, compliance, and information management framework and supports the secure, lawful, and transparent handling of personal data in institutional decision-making and regulatory reporting.

This Data Protection Policy aligns with OfS Condition F1 (Provision of Information) by ensuring that all information provided to the Office for Students, students, and other stakeholders is accurate, complete, timely, and supported by appropriate validation and approval processes. The policy establishes clear responsibilities for data ownership, verification, and reporting, thereby supporting the integrity of statutory returns, regulatory submissions, and published institutional information.

The policy supports OfS Condition F2 (Information Controls) through the implementation of robust data governance and system controls, including secure storage, controlled access, data backup arrangements, audit trails, and regular system reviews. These measures ensure that institutional information systems are reliable, resilient, and protected against unauthorised access, loss, or misuse, thereby supporting effective regulatory reporting and internal decision-making.

This policy aligns with OfS Condition C1 (Consumer Protection Law) by ensuring that students and applicants are provided with clear, accessible, and accurate information regarding the collection, processing, retention, and sharing of personal data. It supports transparency in institutional communications, privacy notices, and contractual documentation, and ensures that individuals are informed of their data rights and how these may be exercised.

The policy supports OfS Condition C5 (Treating Students Fairly) by ensuring that personal data is processed lawfully, consistently, and without discrimination. It promotes equitable treatment in academic administration, support services, and decision-making processes by safeguarding the accuracy, confidentiality, and appropriate use of student records and personal information.

This policy aligns with OfS Condition E1 (Public Interest Governance) by embedding data protection within LAAT's governance framework and ensuring that senior leaders and governing bodies receive regular assurance on information security, compliance, and regulatory risk. Oversight arrangements support transparency, ethical data management, and accountability in the public interest.

The policy supports OfS Condition E2 (Management and Governance) through clearly defined roles, responsibilities, and reporting structures for data protection and information governance. It ensures that management arrangements are proportionate to institutional risk and complexity and that data compliance is systematically monitored, reviewed, and integrated into operational and strategic planning.

This policy aligns with OfS Condition E3 (Accountability) by establishing formal accountability mechanisms for data protection compliance, including named policy owners, system custodians, and senior managers. It supports documented decision-making, incident reporting, breach management procedures, and internal audit activity to evidence institutional responsibility for regulatory compliance

Terms of Reference

1. Purpose

This policy sets out how LAAT manages the processing of personal data in relation to its higher education provision and other operations. It establishes standards and responsibilities for staff and students to ensure compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. It provides a framework for processing personal data lawfully, fairly, and transparently.

2. Scope

- **Who:** All staff employed by LAAT, all students enrolled on franchised or partnered programmes, and any agency staff, contractors, and visitors who process LAAT personal data.
- **What:** All activities involving the collection, storage, processing, sharing, or disposal of personal data relating to students, staff, and stakeholders.
- **Where:** All LAAT campuses and approved online or blended learning platforms.

Note: This policy does not apply to personal data processing carried out under the direct control of a validating university or partner institution where that institution is the data controller. In such cases, the partner's data protection policy takes precedence.

3. Definitions

- **Personal Data:** Information relating to an identified or identifiable natural person.
- **Processing:** Any operation performed on personal data (e.g., collection, storage, use, disclosure, deletion).
- **Data Subject:** An individual to whom personal data relates.
- **Data Controller:** The natural or legal person that determines the purposes and means of processing personal data.
- **Data Processor:** A natural or legal person that processes personal data on behalf of a data controller.

4. Principles

LAAT applies the six data protection principles set out in the UK GDPR. Personal data must be:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified and legitimate purposes.
3. Limited to what is necessary.
4. Accurate and kept up to date.
5. Stored only for as long as necessary.
6. Processed in a manner that ensures appropriate security.

In addition, LAAT adopts the following guiding principles:

- **Accountability:** Responsibilities are clearly defined, and evidence of compliance is maintained.
- **Student and People-centred practice:** The rights, privacy, and wellbeing of data subjects are central to decision-making.
- **Inclusivity and accessibility:** Data protection processes are applied consistently to all individuals, regardless of status.
- **Compliance and proportionality:** Controls are proportionate to the sensitivity and volume of the data processed.

5. Governance, Committees and Terms of Reference

5.1 Governance and Oversight

Overall governance for data protection is provided by the Board of Governors in line with OfS Condition E2. The **Audit & Risk Committee** has primary responsibility for overseeing the implementation and effectiveness of this policy. Other committees that may receive reports include the Academic Board and the People & Culture Committee.

5.2 Oversight Committee – Terms of Reference (Extract)

The Audit & Risk Committee will approve and periodically review this policy, monitor compliance with regulatory requirements, review incident data and annual reports, recommend improvements to mitigate risks, and report annually to the Board of Governors on key issues arising from data protection.

6. Policy Statement

6.1 Lawful Processing

All personal data processed by LAAT must have a valid legal basis under the UK GDPR. Data processing must be limited to the purposes for which it was collected and performed in a fair and transparent manner. Consent must be obtained where required.

6.2 Data Security

Appropriate technical and organisational measures must be implemented to protect personal data against unauthorised access, accidental loss, or destruction. Data should be pseudonymised or encrypted where feasible. Staff must follow the **Information Security Policy** for system-level controls.

6.3 Data Breach Reporting

Suspected or actual personal data breaches must be reported **immediately** to the Data Protection Officer (DPO). LAAT will investigate breaches and, where necessary, notify the Information Commissioner's Office (ICO) and affected individuals without undue delay.

6.4 Training and Awareness

All staff and students handling personal data must complete mandatory data protection training and refresh it every two years.

6.5 Data Sharing

Personal data may only be shared with third parties where there is a lawful basis, and appropriate data sharing agreements are in place. Departments are required to plan ahead and ensure data sharing agreements are executed prior to the transfer of any data to ensure safe and timely sharing.

7. Standard Operating Procedure – Overview

Appendix A sets out the detailed procedure for planning, communicating, processing, escalating, and recording personal data handling activities. It includes guidance on completing data protection impact assessments (DPIAs), maintaining records of processing activities, and responding to data breaches.

8. Monitoring, Compliance and Review

The Data Protection Officer will monitor compliance through annual reports, audits, and training completion records. Non-compliance may lead to HR processes or disciplinary measures. The policy will be reviewed every two years or sooner if required by changes in legislation or partner requirements.

9. Responsible People / Roles include

- **Policy Owner (Head of IT): Mr Himanshu Chadha**
  Maintains and reviews the policy, ensures alignment with legislation, provides leadership on implementation, and reports to the Audit, Risk and Finance Committee.
- **Register: Mr Stephen Plant**
  System security, access control, data accuracy and integrity.
- **Data Protection Officer: Nadia Asim**
  The Data Protection Officer oversees institutional compliance with data protection legislation and regulatory requirements and provides guidance and support to staff.
- **All Staff:** Comply with the policy, complete mandatory training, and report breaches or risks.
- **Students:** Follow guidance in student handbooks and use appropriate channels to raise concerns.

List of people and contact

Role	Name	Contact email
Head of IT	Himanshu Chadha	himanshu@laat.ac.uk
Register	Stephen Plant	stephen.plant@laat.ac.uk
Data Protection Officer	TBC	TBC

10. List of Documents

- Data Protection Impact Assessment (DPIA) Template
- Data Breach Reporting Form
- Data Subject Access Request (DSAR) Log
- Third-Party Data Processing Agreement (Standard Clause)
- Data Subject Access Request Policy
- Information Security Policy
- Safeguarding and Prevent Policy

11. Evidence

- Data Protection Impact Assessment (DPIA) Template
- Data Breach Reporting Form
- Data Subject Access Request (DSAR) Log

- Third-Party Data Processing Agreement (Standard Clause)
- Data Subject Access Request Policy
- Information Security Policy
- Safeguarding and Prevent Policy

Evidence Item	**Purpose / What it Demonstrates**	**Relevant OfS Condition(s)**
Data Protection Impact Assessment (DPIA) Template	Demonstrates structured assessment and mitigation of data protection risks before new or high-risk processing activities are implemented	F2 (information controls), E2 (management and governance), E3 (accountability)
Data Breach Reporting Form	Provides a formal mechanism for recording, escalating, and managing personal data breaches	F2 (information controls), E3 (accountability), E2
Data Subject Access Request (DSAR) Log	Evidences compliance with individual rights and transparency in responding to access requests	C1 (consumer protection), C5 (fair treatment), E3
Third-Party Data Processing Agreement (Standard Clause)	Demonstrates control and oversight of outsourced data processing and contractual compliance	F2 (information controls), C1 (consumer protection), E3
Data Subject Access Request Policy	Establishes formal procedures for handling subject access requests lawfully and consistently	C1 (consumer protection), C5 (fair treatment), E2
Information Security Policy	Confirms technical and organisational safeguards to protect institutional data systems	F2 (information controls), E2 (management and governance)
Safeguarding and Prevent Policy	Demonstrates secure and lawful handling of sensitive student information in welfare and safeguarding contexts	C5 (fair treatment), B2 (resources, support and engagement), E2

Appendix A – Standard Operating Procedure (SOP)

Scope: This SOP provides step-by-step guidance for staff on identifying lawful bases, completing impact assessments, securing data, handling third-party contracts, and managing breaches.

A1. Lawful Basis for Processing

Before starting any new project or administrative process involving personal data, staff must identify a lawful basis.

1. **Check:** Does the processing fall under Contract, Legal Obligation, Vital Interests, Public Task, or Legitimate Interests?
2. **Consent:** If none of the above apply, you may need explicit Consent.
3. **Documentation:** Record the decision in the project initiation document.

A2. Data Protection Impact Assessments (DPIA)

A DPIA is mandatory for high-risk processing (e.g., using new technologies, processing special category data like health records, or large-scale student monitoring).

1. **Download:** Retrieve the DPIA Template from the IT Teams Channel.
2. **Complete:** Fill in the nature, scope, context, and purposes of processing.
3. **Submit:** Send to the DPO (Head of IT) for review *before* processing begins.

A3. Data Security & Storage

- **Storage:** Store personal data only on approved LAAT platforms (e.g., OneDrive, Teams, VLE). **Never** save personal data to local C: drives or unencrypted USB sticks.
- **Email:** When emailing personal data externally, ensure the file is password protected or encrypted.
- **Clear Desk/Screen:** Lock screens when away from your desk. Do not leave paper records containing student data on desks overnight.

A4. Managing Data Breaches

A breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Immediate Steps for Staff:

1. **Contain:** Attempt to stop the breach (e.g., recall the email, isolate the infected computer).
2. **Report:** Notify the DPO immediately via email (Subject: URGENT DATA BREACH) or phone.
    a. *Time is critical: The DPO has 72 hours to report serious breaches to the ICO.*
3. **Details:** Provide the DPO with: What happened? When? What data is involved? How many people are affected?

A5. Third-Party Data Sharing

1. **Contracts:** Never share data with a new software provider or agency without a signed Data Processing Agreement (DPA).
2. **Verification:** Check the "Approved Suppliers List" on the IT Teams Channel. If the supplier is not there, contact IT to initiate a vendor security check.

A6. Forms and Templates

The following templates are available on the **LAAT IT TEAMS CHANNEL** and the **VLE**:

- DPIA Template
- Data Breach Reporting Form
- Data Subject Access Request (DSAR) Log
- Third-Party Data Processing Agreement (Standard Clause)