London Academy for Applied Technology

Data Subject Access Request (DSAR) Policy

Document reference: LAAT-IT-POL-002
Department / Function: IT
Owner: Data Protection Officer, Himanshu Chadha
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

Regulatory Alignment with Office for Students (OfS) conditions

This Data Subject Access Policy forms part of the London Academy for Applied Technology's (LAAT) governance and information management framework and supports transparency, accountability, and lawful handling of personal data in line with institutional regulatory arrangements.

The policy aligns with OfS Condition C1 (Consumer Protection) by ensuring that students and staff are provided with clear, accurate, and accessible information regarding their rights to access personal data and the procedures for submitting subject access requests. It also supports Condition C5 (Treating Students Fairly) by promoting fair, consistent, and timely handling of requests, thereby ensuring equitable treatment in institutional decision-making and information provision processes.

The policy further aligns with OfS Condition E1 (Public Interest Governance) and Condition E3 (Accountability) by establishing clear roles, responsibilities, and oversight arrangements for data protection compliance within LAAT's governance structure. It contributes to effective institutional oversight by embedding data protection responsibilities within senior management and reporting frameworks. In addition, the policy supports Condition F2 (Information Controls) by ensuring that information systems, records management, and data handling practices are reliable, secure, and subject to appropriate internal controls, as outlined in the OfS Conditions of Registration framework.

Through regular monitoring, staff training, and integration within LAAT's wider compliance and quality assurance framework, this policy ensures that data subject access rights are upheld in accordance with legal and regulatory requirements. It

supports continuous improvement, regulatory assurance, and the protection of student and stakeholder interests.

Terms of Reference

1. Purpose

This policy establishes how LAAT will recognise and respond to Data Subject Access Requests (DSARs) made under Article 15 of the UK GDPR. Article 15 gives data subjects the right to obtain confirmation as to whether or not personal data concerning them is being processed and, where that is the case, access to that data and information about the processing gov.uk. LAAT is committed to ensuring that DSARs are handled lawfully, transparently and within statutory timescales, thereby protecting individuals' rights and promoting trust in LAAT's data practices.

2. Scope

- **Who**: Any individual whose personal data is processed by LAAT, including students, applicants, alumni, staff, contractors and visitors.
- **What**: All requests to access personal data held by LAAT, regardless of format (verbal, written, electronic or via authorised representatives).
- **Where**: All LAAT campuses, systems, paper records and authorised third party processors.

This policy does not apply to requests for information under the Freedom of Information Act 2000; such requests are handled via separate procedures.

3. Definitions

- **Data Subject Access Request (DSAR)** – a request made by or on behalf of an individual for access to personal data and supplementary information that a controller holds about them.
- **Verification** – process of validating the identity of the requester to ensure data is disclosed only to the rightful individual.
- **Exemption** – specific circumstances under which certain personal data may be withheld from disclosure (e.g. legal privilege, third party confidentiality).

4. Principles

1. **Accessibility** – DSAR procedures will be clearly described and accessible to all individuals.
2. **Timeliness** – LAAT will respond to DSARs without undue delay and within one calendar month of receipt; this timeframe may be extended by up to two months for complex requestsgov.uk.

3. **Security and Confidentiality** – identity verification is mandatory before releasing any personal data to ensure disclosure to the correct person.
4. **Transparency** – requesters will be informed of the status of their request, reasons for any refusal, and their right to complain to the ICO.
5. **Accountability** – LAAT will maintain records of all DSARs and responses to demonstrate compliance.

5. Governance, Committees and Terms of Reference

Overall governance is provided by the Board of Governors. The Audit, Risk & Finance Committee oversees the DSAR process, ensuring it meets legislative requirements and reviewing annual metrics on response times, volume and outcomes.

6. Policy Statement

6.1 Submitting a DSAR

Requests may be made verbally or in writing (including via email or designated online forms). Staff receiving a request must immediately notify the DPO. The DPO records the receipt date and confirms whether the request is valid.

6.2 Identity Verification

The DPO will verify the requester's identity using appropriate identification documents or existing authentication credentials before processing the request. If identity is not established, LAAT may refuse or request further proof.

6.3 Clarifying the Request

If the request is broad, the DPO may ask the requester to specify the information sought to narrow the scope and facilitate timely retrieval.

6.4 Gathering Information

Departments must search all relevant systems, files and archives to identify personal data. Third-party processors will be contacted where necessary.

6.5 Response and Delivery

The response will be provided within one calendar month, including copies of personal data and details of processing activities, unless an extension is justified under the UK GDPR. Data will be provided in a secure format.

6.6 Exemptions

Certain information may be withheld if an exemption applies (e.g. data about other individuals). In such cases, the DPO will explain the basis for withholding.

6.7 Complaints

If a requester is dissatisfied, they may raise a complaint with the DPO. If unresolved, they may lodge a complaint with the ICO.

7. Standard Operating Procedure – Overview

Appendix A provides detailed steps for receiving, logging, verifying, retrieving, redacting and responding to DSARs, including templates for acknowledgement letters and response letters.

8. Regulatory, Partner and Legal Alignment

This policy aligns with Article 15 of the UK GDPR gov.uk, the Data Protection Act 2018, and ICO guidance on subject access requests. Partner university policies are observed where LAAT processes data on their behalf.

9. Monitoring, Compliance and Review

The DPO maintains a register of DSARs and monitors response times and outcomes. Metrics are reported annually to the Audit, Risk and Finance Committee. Non-compliance may result in disciplinary action. The policy will be reviewed every two years or sooner if laws or partner requirements change.

10. 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 (DPO): Ms Nadia Asim**
  coordinates DSAR handling, ensures procedures are followed, maintains logs and reports to the Audit, Risk and Finance Committee.
- **Departmental DSAR Coordinators** – designated contacts in each department to assist with locating relevant data.
- **All Staff** – promptly forward any DSARs received to the DPO, cooperate in retrieving data and undertake DSAR training.
- **Requesters** – provide sufficient information to identify themselves and the data sought.

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	Nadia Asim	nadiaasim@laat.ac.uk

11. List of Documents

- Data Subject Access Request Form
- DSAR acknowledge letter
- Identity verification record
- Complaints Handling Procedure
- DSAR final response letter
- Data Protection Policy
- Information Security Policy

12. Evidence

- Data Subject Access Request Form
- DSAR acknowledge letter
- Identity verification record
- Complaints Handling Procedure
- DSAR final response letter
- Data Protection Policy
- Information Security Policy

Mapping table for evidence items related to OfS conditions

Evidence Item	**Purpose / What it Demonstrates**	**Relevant OfS Condition(s)**
Data Subject Access Request Form	Provides students and staff with a clear and accessible mechanism to submit subject access requests	C1 (consumer protection), C5 (fair treatment), E2 (management and governance)
DSAR Acknowledgement Letter	Confirms receipt of requests and communicates statutory timescales and processes	C1 (consumer protection), C5 (fair treatment), E3 (accountability)
Identity Verification Record	Demonstrates secure verification of applicant identity prior to data disclosure	F2 (information controls), E2 (management and governance), E3 (accountability)
Complaints Handling Procedure	Establishes formal procedures for raising and resolving	C1 (consumer protection), C5 (fair treatment), E2

	complaints, including data-related concerns	(management and governance)
DSAR Final Response Letter	Provides formal confirmation of disclosure decisions and information supplied	C1 (consumer protection), C5 (fair treatment), E3 (accountability)
Data Protection Policy	Provides overarching framework for lawful, secure, and transparent data processing	F1 (information provision), F2 (information controls), E2 (management and governance)
Information Security Policy	Confirms technical and organisational safeguards to protect personal and institutional data	F2 (information controls), E2 (management and governance)

Appendix A – SOP: DSAR Handling

This appendix outlines the detailed process for each stage of a DSAR, including forms for acknowledgement, checklists for locating data, guidelines for redaction and secure transmission, and recordkeeping requirements.

Standard Operating Procedure (SOP)

1. Purpose of this SOP

This Standard Operating Procedure (SOP) defines the mandatory, step-by-step process for receiving, managing, responding to and closing Data Subject Access Requests (DSARs) at LAAT. It ensures that all DSARs are handled lawfully, consistently, securely and within statutory timescales in line with Article 15 of the UK GDPR and the Data Protection Act 2018

2. Scope

This SOP applies to:

- All DSARs received by LAAT, regardless of format (verbal, written, email, online form or via an authorised representative)
- All LAAT staff involved in receiving, processing or responding to DSARs
- All personal data held by LAAT, including electronic systems, paper records and third-party processors

This SOP does **not** apply to Freedom of Information (FOI) requests.

3. Roles and Responsibilities

3.1 Data Protection Officer (DPO)

- Acts as the single point of contact for all DSARs
- Validates and logs requests
- Verifies identity of requesters
- Coordinates data searches across departments
- Reviews exemptions and redactions
- Issues formal responses
- Maintains DSAR records and metrics

3.2 Departmental DSAR Coordinators

- Conduct searches of departmental systems and records
- Complete DSAR Data Search Checklists
- Return data securely and within agreed deadlines

3.3 All Staff

- Recognise DSARs in any format
- Immediately forward DSARs to the DPO
- Cooperate fully with data searches and timelines

3.4 Requesters (Data Subjects)

- Provide sufficient information to verify identity
- Clearly describe the data requested, where possible

4. DSAR Handling Procedure

Step 1: Receipt of a DSAR

1. A DSAR may be received verbally, in writing, by email or via an online form.
2. Any staff member receiving a DSAR must forward it to the DPO **within one working day**.
3. The DPO records the request in the DSAR Register, noting:
    a. Date received
    b. Requester name
    c. Method of receipt
    d. Initial deadline (one calendar month)

Step 2: Acknowledgement

1. The DPO issues a written acknowledgement to the requester within **5 working days**.
2. The acknowledgement confirms:
    a. Receipt of the DSAR
    b. The statutory response deadline
    c. Any requirement for identity verification

(Form DSAR-01 – Acknowledgement Letter)

Step 3: Identity Verification

1. The DPO verifies the identity of the requester before any data is disclosed.
2. Acceptable verification methods include:
    a. Existing LAAT authentication credentials
    b. Photographic ID plus proof of address
    c. Authorisation documents where acting via a representative
3. If identity cannot be verified, processing is paused until sufficient evidence is provided.

(Form DSAR-02 – Identity Verification Record)

Step 4: Clarification (if required)

1. If a request is broad or unclear, the DPO may seek clarification.
2. The statutory deadline is paused until clarification is received.
3. All correspondence is logged in the DSAR Register.

Step 5: Data Search and Retrieval

1. The DPO issues a Data Search Request to relevant departments.
2. Departments must:
    a. Search all relevant systems, files and archives
    b. Include emails, databases, shared drives and paper files
    c. Return results by the specified internal deadline
3. Third-party processors are contacted where applicable.

(Form DSAR-03 – Departmental Data Search Checklist)

Step 6: Review, Redaction and Exemptions

1. The DPO reviews all retrieved data.
2. Data is assessed for:
    a. Accuracy and relevance

    b. Third-party personal data
    c. Legal or statutory exemptions
3. Redactions are applied where required, with reasons documented.

(Form DSAR-04 – Exemption and Redaction Log)

Step 7: Response Preparation and Delivery

1. The DPO prepares the formal DSAR response, including:
    a. Confirmation of processing
    b. Copy of personal data
    c. Purposes of processing
    d. Data categories and recipients
    e. Retention periods
    f. Data subject rights
2. Data is provided securely (encrypted email, secure portal or registered post).
3. The response is issued within **one calendar month**, unless an extension applies.

(Form DSAR-05 – Final Response Letter).

Step 8: Extension of Time (if applicable)

1. For complex or multiple requests, the deadline may be extended by up to two months.
2. The requester must be informed in writing within the original one-month period, including reasons for the extension.

Step 9: Closure and Recordkeeping

1. Once the response is issued, the DPO:
    a. Updates the DSAR Register
    b. Records completion date and outcome
    c. Retains records for audit and compliance purposes
2. DSAR records are retained in line with LAAT's retention schedule.

Step 10: Complaints and Escalation

1. If dissatisfied, requesters may complain to the DPO.
2. If unresolved, they may escalate to the Information Commissioner's Office (ICO).
3. All complaints are logged and reported to the Audit, Risk & Finance Committee.

5. Monitoring and Reporting

- The DPO reviews DSAR metrics annually, including:

    - Number of requests received
    - Response times
    - Extensions applied
    - Complaints received
- Metrics are reported to the Audit & Risk Committee.

6. Forms and Templates

DSAR-01 – DSAR Acknowledgement Letter

DSAR-02 – Identity Verification Record

DSAR-03 – Departmental Data Search Checklist

DSAR-04 – Exemption and Redaction Log

DSAR-05 – DSAR Final Response Letter

(Standard templates are maintained by the DPO and reviewed biennially.)

7. Related Documents

- Data Subject Access Request (DSAR) Policy (LAATITPOL002)
- Data Protection Policy
- Information Security Policy
- Complaints Handling Procedure
- ICO Guidance on Subject Access Requests

Appendix B – DSAR Forms and Templates

DSAR-01 – Data Subject Access Request Acknowledgement Letter

To: [Requester Name]
Address / Email: [Requester Contact Details]
Date: [Date]
Subject: Acknowledgement of Data Subject Access Request
Dear [Requester Name],
We acknowledge receipt of your Data Subject Access Request (DSAR) received on **[date]**.
LAAT is processing your request in accordance with Article 15 of the UK General Data Protection Regulation (UK GDPR). We aim to provide our response no later than **[deadline – one calendar month from receipt]**, subject to verification of your identity.
To enable us to proceed, please provide the following identification documents (if not already supplied):

- Proof of identity (e.g. passport or driving licence)
- Proof of address (dated within the last 3 months)

If you have any questions regarding this process, please contact the Data Protection Officer at **[DPO email]**.

Yours sincerely,

Data Protection Officer

LAAT

DSAR-02 – Identity Verification Record

DSAR Reference Number: [DSAR-XXXX]

Requester Name: [Full Name]

Verification Item	Provided (Y/N)	Verified By	Date Verified
Photo ID			
Proof of Address			
LAAT Credentials			
Authorisation (if representative)			

Verification Outcome:

☐ Identity verified – proceed with request

☐ Further information required (details below)

Notes:

[Free text]

DPO Name & Signature: _____

Date: _____

DSAR-03 – Departmental Data Search Checklist

DSAR Reference Number: [DSAR-XXXX]

Department: [Department Name]

Coordinator: [Name]

Systems and Records Searched (tick all that apply):

- ☐ Student Records System
- ☐ HR / Staff Records
- ☐ Email Accounts
- ☐ Shared Drives
- ☐ Learning Platforms (VLE, Teams, etc.)
- ☐ Paper Files
- ☐ Third-Party Systems
- ☐ Other (specify): _____

Data Located:

☐ Yes (attached securely)

☐ No personal data found

Date Search Completed: _____

Coordinator Signature: _____

DSAR-04 – Exemption and Redaction Log

DSAR Reference Number: [DSAR-XXXX]

Data Item	Exemption Applied	Legal Basis	Redaction Method	Approved By

Summary Explanation Provided to Requester:

[Free text]

DPO Approval Signature: _____

Date: _____

DSAR-05 – Final DSAR Response Letter

To: [Requester Name]

Date: [Date]

Subject: Response to Your Data Subject Access Request

Dear [Requester Name],

Further to your Data Subject Access Request dated **[date]**, please find enclosed the personal data held by LAAT relating to you.

In accordance with Article 15 of the UK GDPR, this response includes:

- Confirmation that your personal data is processed
- Copies of your personal data
- Purposes of processing
- Categories of personal data
- Recipients of the data
- Retention periods
- Your rights under data protection law

Certain information has been withheld or redacted where legally permitted. Where applicable, explanations have been provided.

If you are dissatisfied with this response, you may contact the Data Protection Officer at **[DPO email]**. You also have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Yours sincerely,

Data Protection Officer

LAAT

End of SOP