Student Data Protection Policy

Version 7.0

Approved by the Board of Governors

Last Amendment: October 2026

This policy sets out the obligations of the London School of Science and Technology Ltd. ("LSST", "the School") regarding data protection and the rights of students, customers, business contacts and other users ("data subjects") in respect of their personal data. Staff should refer also to the *Employee Data Protection Policy*.

This policy has been aligned to the following legislation:

i. UK GDPR (as supplemented by the Data Protection Act 2018)

DOCUMENT INFORMATION

Document owner(s)*: Data Security Officer

Date of next review: September 2027

Document Status: Approved

Dissemination: For general publication

*The document owner is responsible for maintaining and updating the content of this document and ensuring that it reflects current practice at the School.

Contents

DOCUMENT INFORMATION 1
1. INTRODUCTION 3
1.6. Under the GDPR, personal data must: 4
2. YOUR RIGHTS 4
3. HOW WE USE YOUR DATA 6
4. CONFIDENTIALITY 9
5. STAFF RESPONSIBILITIES 9
6. STUDENT RESPONSIBILITIES 10
7. STUDENTS WITH DISABILITIES OR DYSLEXIA 10
8. SUBJECT ACCESS 10
9. RETENTION OF RECORDS 10
9.3. Table of Retention: 11
10. REPORTING AND MANAGING SUSPECTED DATA BREACHES 12
10.1. Purpose 12
10.2. Definition of a Data Breach 12
10.3. Staff Responsibilities 13
10.4. Reporting a Suspected Breach 13
10.5. Investigation and Response 14
10.6. Document Sharing and Access Protocol 14
10.7. Non-Compliance and Disciplinary Action 14
10.8. Related Policies and Documents 15
11. KEY CONTACT DETAILS 15
12. THIRD PARTY ACCESS TO STUDENT DATA 15
13. STUDENT CONSENT AND OPT-OUT OPTIONS 16
APPENDIX A: SUBJECT ACCESS REQUEST FORM 17
APPENDIX B: LSST DATA BREACH REPORTING FORM 22

VERSION HISTORY 25

1. INTRODUCTION

1.1. As a centre for education, much of the School's work is concerned with information and its use. For both educational and administrative purposes, LSST needs to collect and retain personal data about its students to allow it to operate effectively and efficiently, for example to register students, monitor performance, to ensure their health and safety and to monitor equal opportunities.

1.2. Personal data is recorded information that relates to a living person that can be associated with that person, either from other information in the possession of the organisation holding the data or by cross referencing to information held by a third party. This includes expressions of opinion about the individual and indication of any intentions of the Data Controller or any other person in regard to the individual. Recorded information can be stored electronically or in a manual filing system.

1.3. Examples of Personal Data include:

- Name, home and work addresses.
- Telephone number and email address.
- IP address and username.
- Date of birth and gender.
- Civil/Marital status.
- National insurance and passport numbers.
- Bank account or credit card details.
- Criminal offence details.
- Insurance policy details.
- Employment records.
- Right to work/VISA details.
- National, racial/ethnic origin.
- Education history including qualification details.
- Images caught on close circuit television (CCTV).
- Student record information.
- Student exam results.

1.4. To comply with the law, such personal data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The principles to ensure that personal data is processed properly, and which the School follows to ensure it complies with the legislation, are set out in the UK GDPR and the Data Protection Act 2018, available on the Information Commissioner's Office website (www.ico.gov.uk).

1.5. LSST is committed not only to legal compliance but also to upholding the highest ethical standards in the handling of student data. We value transparency, accountability, and respect for individual privacy in all aspects of our operations.

1.6. Under the GDPR, personal data must:

1.6.1. Be processed fairly and lawfully.

1.6.2. Be obtained for a stated purpose(s) and not processed for anything other than the stated purpose(s) and for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

1.6.3. Be adequate, relevant and not excessive for the purpose for which it was obtained.

1.6.4. Be accurate and be kept up to date and, if inaccurate, be rectified or erased without delay.

1.6.5. Not be kept for longer than is necessary for the purpose for which it was obtained except where anonymised so that the individual cannot be identified.

1.6.6. Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.7. LSST will ensure that these principles are always followed. Through appropriate management and strict application of criteria and controls, LSST will process personal data only as set out in this policy and the LSST Privacy Notice.

1.8. If a data breach occurs, clear procedures will be followed to assess the impact, contain the issue, and notify affected individuals and relevant authorities as required by law. This ensures transparency and prompt action to mitigate risks.

2. YOUR RIGHTS

2.1. To exercise any of your data rights, students may submit a request to the Registry via registry@lsst.ac. LSST will respond to valid requests within one calendar month, or inform the requester of any delay. The Subject Access Request Form can be found under Appendix A.

2.2. The GDPR provides the following rights for individuals:

- **Informed**: The right to be informed about the collection and use of personal data is addressed via company privacy notes.

- **Subject access:** The right to request information about how personal data is being processed, including whether personal data is being processed, the right to be allowed access to that data, to be provided with a copy of that data, along with the right to obtain the following information:

    - The purpose of the processing.

    - The categories of personal data.

    - The recipients to whom data have been disclosed or which will be disclosed.

    - The retention period.

    - The right to lodge a complaint with the Information Commissioner's Office.

    - The source of the information if not collected direct from the subject.

    - The existence of any automated decision-making.

- **Rectification:** The right to allow a data subject to rectify inaccurate personal data concerning them.

- **Erasure:** The right to have data erased and to have confirmation of erasure, but only where:

    - The data is no longer necessary in relation to the purpose for which it was collected.

    - Where consent is withdrawn.

    - Where there is no legal basis for the processing.

    - There is a legal obligation to delete data.

- **Restriction of processing:** The right to ask for certain processing to be restricted in the following circumstances:

    - If the accuracy of the personal data is being contested.

    - If our processing is unlawful but the data subject does not want it erased.

    - If the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise, or defence of legal claims.

    - If the data subject has objected to the processing, pending verification of that objection.

- **Data portability:** The right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if LSST was processing the data using consent or based on a contract.

- **Object to processing:** The right to object to the processing of personal data relying on the legitimate interests processing condition unless LSST can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

- **Object to automated profiling:** The right to object where solely automated decision-making is being carried out that has legal or similarly significant effects on the data subject. Students have the right to request human intervention, express their views, and challenge decisions.

2.3. Students can exercise these rights by submitting a written request to LSST's Data Protection Officer. Requests will be reviewed in line with legal obligations, and responses will be provided within the required timeframe.

2.4. Further information on how these rights can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

3. HOW WE USE YOUR DATA

3.1. LSST may use and process personal data (including Special Category and criminal offence data) or information regarding you whilst you are a student of LSST and after you have left LSST. Special Category data includes information held by LSST as to your physical or mental health or condition, your racial/ethnic origin, sexual orientation/sex-life, political views, or religion. Criminal offence data includes information on the commission or alleged commission of any offence by you and any proceedings for an offence committed or alleged to have been committed by you (including the outcome or sentence in such proceedings).

3.2. We may obtain the following categories of personal data from third-parties:

- Identifying data e.g. usernames, names, email addresses.

- Tracking data e.g. attendance records taken by contractor lecturers.

- Financial data e.g. payment and student finance data collected by contractor finance staff.

- Medical and health information e.g. sick notes.

- Professional e.g. employer or past academic references, academic record information for SAPE.

- Criminal e.g. enhanced DBS checks for health and social care courses.

3.3. LSST processes your data, including Special Category Data for the purposes and in the manner set out in its Privacy Notice. The processing of your personal data for the below purposes is required for the performance of the contract between you and LSST, for LSST to meet its regulatory obligations to the OfS and for LSST's legitimate interests including marketing, quality assurance and ensuring safety and security of staff and students. We may also ask for your consent for participation in some marketing activities (e.g. subscribing to marketing information along with our newsletter). In those instances, you have the right to withdraw such consent at any time.

3.4. The purposes for which LSST may process your personal data (including Special Category data) include:

- The administration of your enrolment and participation on a course, including the administration of examinations, the issuance of results and certificates in connection with the course, where applicable, the provision to your employer or other sponsor/corporate sponsor information about your attendance and performance on a course and DBS checking where this is required for a course.

- The provision of LSST services and facilities to you and the protection of your health, safety and welfare whilst at LSST.

- The issue and operation of LSST's ID card in accordance with the conditions of the Student enrolment terms and conditions.

- The collection of tuition fees and other LSST fees.

- Equal opportunities monitoring.

- Arrangement and marketing of alumni activities.

- The provision of references about you.

- The provision of information to any regulator, government body or agency.

- For safety purposes.

- The provision of information to the Higher Education Statistics Agency (HESA).

3.5. Your HESA information including linked data is used for broad purposes: public functions, administrative uses, HESA publications, equal opportunity, research, journalism and other processing in which there is a legitimate interest. For more information see the HESA Collection Notice on http://www.hesa.ac.uk/fpn

3.6. In some circumstances, it may be necessary for LSST to transfer your personal data to a country outside the UK (for example, if that is your country of origin). Such a transfer will only be made for the purposes specified above.

3.7. You should be aware that countries outside the UK may not offer data protection law equivalent to that applicable in the United Kingdom and you consent to the transfer of data in these circumstances and for those purposes. Where we make such a transfer to a country that does not provide the same level of data protection as the UK, we will put appropriate measures in place to ensure your information is protected:

- Standard contract clauses.
- International Data Transfer Agreement.
- Binding corporate rules.
- Adequacy decision.
- An exception as defined in Article 49 of the GDPR.

3.8. In some circumstances your personal data will be processed by a third party on our behalf – e.g. a work placement provider, a student recruitment agency or contractor lecturing or administrative staff. Any such processing will only be done under a GDPR compliant processor contract requiring the third-party to only process the data in accordance with our written instructions.

3.9. LSST collects, processes and stores criminal offence data about past convictions, including enhanced DBS check reports from APCS, details of unspent convictions and DBS certificates. This is required for the performance of your contract of enrolment with the School for Health & Social Care courses. This is also required for the legitimate interest of protecting the safety of staff, students and visitors of the School. We do not keep a comprehensive record of criminal offence data.

3.10. Your data will be received by the following categories of third-party recipients:

- Awarding bodies.
- Regulators and funding agencies.
- Debt recovery agencies instructed to recover outstanding fees.
- Contractor staff.
- Partner course and skill providers.
- Professional advisors, e.g., our accountants, legal representatives, quality assurance consultants, our DPO.
- Public authorities and law enforcement, e.g., HESA, the police, UKVI.

3.11. LSST may make video and/or audio recordings of face-to-face and online lectures for training and quality monitoring purposes, which may include students' contributions to classroom discussions and expressions of opinion. These recordings may also be used

by the School for investigating suspected instances of misconduct or breaches of security.

3.12. Further to 3.11., in some circumstances, LSST may use data in the form of photographs or video or audio recordings, of classroom settings as part of general marketing materials, for example, in LSST's annual report, prospectus or course materials. Video and audio recordings and any personal data alongside them will only be used in this way with your explicit consent, which you have the right to withdraw at any time.

3.13. If LSST does not process your data fairly, you may lodge a complaint with the Information Commissioners Office (ICO) here: https://ico.org.uk/concerns/handling/ within 3 months of your last contact concerning the matter with LSST (or such other time limit as the ICO specifies).

4. CONFIDENTIALITY

4.1. All information given to the School staff will be treated with sensitivity, care and discretion. In most circumstances, the information students provide is treated as confidential, but members of staff may discuss aspects of student enquiry or circumstances with their immediate colleagues or in a few cases where relevant, with the School management. If such discussions take place, it will usually be for the sole purpose of seeking information, confirming the best course of action or helping the member of staff to reflect on their work with you. Whenever possible, any such discussion between School staff will take place without the identification of the student personally.

5. STAFF RESPONSIBILITIES

5.1. Staff whose work involves the use of personal data are responsible for ensuring that:

- Any personal data which they hold whether electronically or in hard copy is kept securely, including using password protection on computer files.
- Personal data is not disclosed by them, either orally or in writing, to any unauthorised third party.
- The personal data is accurate and kept up to date, held for the appropriate length of time and destroyed confidentially when/ if no longer needed.
- They do not access any personal data which is not necessary for carrying out their work.
- Report any data breaches to the DPO within 48 hours where feasible, to enable the School to comply with its obligation to record all data breaches and to report a data breach to the ICO within 72 hours.

5.2. Managers have an additional responsibility to ensure that their staff are aware of the data protection principles and know how to correctly process personal and sensitive personal data as part of their work.

6. STUDENT RESPONSIBILITIES

6.1. It is students' responsibility to inform LSST if their personal details require updating. We will provide an annual opportunity for a student to check their data through the registration process.

6.2. At registration, we also collect the contact details of a person nominated by student for emergency contact purposes. A student must notify them that we are holding this data which will only be used in an emergency.

7. STUDENTS WITH DISABILITIES OR DYSLEXIA

7.1. If a student has declared a disability or dyslexia, the School is legally required under the Equality Act 2010 to make appropriate and reasonable adjustments in order to help such student to participate to the fullest extent possible in the educational opportunities provided by the School. Information about the student's condition and requirements will be limited to that necessary to ensure that appropriate adjustments can be made to help the student gain maximum benefit from their course of study. Any information will normally only be passed to others with the student's agreement.

8. SUBJECT ACCESS

8.1. Students are entitled to request a copy of the data we hold about them. Any person who wishes to exercise this right should complete the '*Subject Access Request'* form available from the Student Portal and submit it to the Registry.

8.2. LSST will comply with requests for access to personal data as quickly as possible and will ensure that it is provided within one month of the receipt of the request. LSST can extend the time to respond by a further two months if the request is complex or it has received a number of requests from the student. LSST will inform the student within 1 month of receiving their request why the extension is necessary.

8.3. Requests made for exam results through a Subject Access Request prior to the publication date for the results or that are intended to compel the release of the transcript of certificates themselves (for example where these have been withheld for failure to pay fees), the request will be treated as manifestly unfounded, will be refused and the student will be informed of the reason

9. RETENTION OF RECORDS

9.1. Data related to applications for courses will be retained for 1 year from the date of the application if enrolment is not successful. We will retain a full student record for 6 years

after a student has left LSST so that we can fulfil our function of providing details of the student's education and references when asked to do so. After 6 years have lapsed, we will keep enough data about students to be able to confirm their qualifications achieved whilst at LSST. At the end of each retention period, data will be securely deleted from digital systems, and physical records will be disposed of via confidential shredding or secure waste disposal services.

9.2. Please refer to table 9.3. below for a detailed breakdown of the retention policy for each record.

9.3. Table of Retention:

INFORMATION STORED	TIMESCALE FOR RETENTION
Student records	
Enquirer data (e.g. telephone enquiries from non- applicants, open day bookings, prospectus requests)	1 year after the enquirer's proposed start date
Student application records which can include references, transcripts of entry qualifications, codes of certificates, offer letters complete with any conditions of offer and scholarships for PhD applicants, responses, visa letters and confirmation of acceptance for studies.	**Applicants who are offered a place, accept and enrol:** 6 years **Applicants who start the application form but do not submit:** current academic year + 1 year **Applicants who are not offered a place, or who are offered a place but do not attend:** current academic year + 1 year
Student file – (including enrolment data, general correspondence, any document pertaining to a student, student references and other misc. student details)	6 years after the year of graduation or date of leaving if earlier.
Student loan applications	1 year from enrolment
Conferment/pass lists	100 years
Hardship fund applications	6 years
Student transcripts	100 years
Placement details – managed across the institution – lead should be with business engagement	6 years after the year of graduation or date of leaving if earlier
Recognition of prior learning, claim forms, assessment and evidence, sample of claims and evidence, summary records of claims and decisions	Retain current academic year + 6 years.
Disclosure and barring service (DBS Certificate) disclosure information	6 years after the year of graduation or date of leaving if earlier
Attendance sign in sheets	6 months

Attendance electronic	1 year (day by day breakdown)
Overall attendance summary	Retain for 6 years after graduation or withdrawal
Disabled student support archive, student and support worker records	Retain for 6 years after graduation or withdrawal
Student Complaints	6 years after last action on case
Student Appeals	6 years after last action on case
Extenuating circumstances – applications	6 years after last action on case
Student disciplinary cases	6 years after last action on case
Fitness to practice records	Retain for 6 years after graduation or withdrawal
Audit files - completed and withdrawn students	6 years

10. REPORTING AND MANAGING SUSPECTED DATA BREACHES

10.1. Purpose

10.1.1. This section outlines LSST's policy and procedures for reporting, assessing, and responding to suspected or actual breaches of student personal data. It supports LSST's compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and LSST's internal obligations to protect the confidentiality, integrity, and lawful processing of all student data.

10.2. Definition of a Data Breach

10.2.1. A personal data breach is defined under Article 4(12) of the UK GDPR as:

> "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

10.2.2. Examples include but are not limited to:

- Sending student data to the wrong recipient.
- Documents containing student information being accessed by unauthorised persons.
- Loss or theft of devices containing personal data.
- Uncontrolled sharing or forwarding of sensitive files across LSST departments or externally.

10.3. Staff Responsibilities

10.3.1. All LSST staff (including contractor staff) must:

- Ensure that student data is shared only with authorised individuals with a legitimate academic or administrative need.
- Never download or forward student data to external recipients or personal devices without appropriate authorisation.
- Immediately report any suspected or known breach using the process outlined below.
- Follow all access restrictions applied to shared documents, including view-only permissions where appropriate.

10.3.2. Failure to follow these responsibilities may result in disciplinary action.

10.4. Reporting a Suspected Breach

10.4.1. Any LSST employee or student who suspects a data breach must act **immediately** by following the steps below:

- **For Staff:**
    1. **Notify the Document Owner** (i.e. the person responsible for issuing or managing the student data document).
    2. **Report the breach to the Data Protection Officer (DPO):**
       Email: DPOsupport@worknest.com (Worknest Limited)
       CC: **registry@lsst.ac, noman.nafees@lsst.ac**
    3. **Include the following information:**
        a. Date and time of the incident.
        b. Description of what occurred.
        c. Type of data involved.
        d. Number of individuals affected (if known).
        e. Actions already taken to contain the breach.
- **For Students:**
    1. Students should report concerns about data privacy or suspected data misuse to:
        a. **Student Support Coordinator** (on their campus), or
        b. **registry@lsst.ac**

2. Students may also contact the DPO directly if they are unsatisfied with the internal handling of their concerns.

10.5. Investigation and Response

10.5.1. Upon receipt of a breach report:

- The DPO will assess the severity and risk of harm.
- If applicable, the breach will be contained and secured.
- A formal record will be created and, where required, the breach will be reported to the **Information Commissioner's Office (ICO)** within 72 hours.
- Affected individuals will be informed if their rights or freedoms are at risk.

10.5.2. Where necessary, internal audits and remedial measures (including staff training or revision of access controls) will be undertaken.

10.6. Document Sharing and Access Protocol

10.6.1. To prevent inappropriate sharing:

- Student data documents may only be **shared with designated staff** (e.g. the staff members selected by the document owner).
- Only those deemed necessary by the document owner will be granted **editing rights.**
- If onward sharing is necessary:
    - The **Document Recipient** must first notify the **document owner.**
    - The approved onward recipients must receive **view-only access**, with **download permissions disabled** unless approved by the document owner.
    - A log of sharing must be maintained.

10.6.2. This applies to all formats including Excel files, SharePoint documents, PDFs, and cloud-based spreadsheets.

10.7. Non-Compliance and Disciplinary Action

10.7.1. Any failure to follow this policy, whether through negligence or deliberate action, will be taken seriously and may result in:

- Formal disciplinary procedures.
- Suspension of access to student data systems.
- Reporting to the relevant professional body (if applicable).

- Referral to external authorities if the breach warrants it.

10.8. Related Policies and Documents

- LSST Student Data Protection Policy (this document).
- LSST Employee Data Protection Policy.
- LSST IT Security Policy.
- GDPR Guidance for Staff (internal).
- Subject Access Request Guidance.

11. KEY CONTACT DETAILS

11.1. Students are entitled to request a copy of the data we hold about them. Any person who wishes to exercise this right should complete the '*Subject Access Request'* form available from the Student Portal and submit it to the Registry.

- **London School of Science and Technology Ltd (Data Controller)**

  Memo House, 1st Floor, Kendal Avenue,
  London,
  W3 0XA

  +44 (0) 208 7953 863
  info@lsst.ac

- **LSST Registry (for students' data Subject Access Requests)**

  registry@lsst.ac

- **Worknest Limited (Data Protection Officer)**

  20 Grosvenor Place, London SW1X 7HN

  DPOsupport@worknest.com

12. THIRD PARTY ACCESS TO STUDENT DATA

12.1. All external contractors or service providers handling student data must:

- Sign a GDPR-compliant Data Processing Agreement (DPA).

- Be pre-approved by the Data Protection Officer.
- Undergo due diligence and periodic compliance checks.

12.2. No access will be granted unless a legitimate purpose is confirmed and appropriate safeguards are in place.

13. STUDENT CONSENT AND OPT-OUT OPTIONS

13.1. Where LSST relies on student consent (e.g. for marketing communications or the use of images/videos in promotional materials), this will be collected explicitly and separately.

13.2. Students have the right to withdraw consent at any time by emailing info@lsst.ac or via the preferences link in any communication.

13.3. No student will be penalised for withholding or withdrawing consent.

APPENDIX A: SUBJECT ACCESS REQUEST FORM

Subject Access Request (Page 1)

Purpose of this form:

It is not mandatory to use this form, but it will help us to give a timely and accurate response to your subject access request as required in the General Data Protection Regulation.

Please complete the table below and return the form by post to London School of Science and Technology, First Floor Memo House, Kendal Avenue, Park Royal, W3 0XA, marked for the attention of Registry: registry@lsst.ac (if you are a student), or HR: hr@lsst.ac (if you are an employee of the School or a contractor).

About you:

Title	
Forename(s)	
Surname	
Other names we may know you by	
Any reference numbers or information that will help us locate the information we hold on you	

How may we contact you? (Provide at least one way):

Telephone	
Email address	
Postal address	

Proving your identity:

We are required to try and verify that you are the person named above. We may ask for one of the following documents – Please tick the ones you could supply:

- ☐ A copy of your passport
- ☐ A copy of your photocard driving licence
- ☐ A copy of alternative recognised photo ID
- ☐ An original utility bill issued in your name

Subject Access Request (Page 2)

Your request:

Please outline the information to which you wish us to provide access:

Subject Access Request (Guidance on Making a Request)

What are your rights?

The Data Protection Act 2018 gives individuals the right to access the personal data that organisations hold about them, subject to certain exemptions (see below). Requests for access to personal data are known as Subject Access Requests (SARs). This guidance explains how to submit a SAR to LSST, how LSST will handle the request and how to complain if dissatisfied.

If a SAR is made to LSST, individuals are entitled to be told whether LSST holds any data about them. If LSST does hold data, the student has the right:

- To be given a description of the data, the purpose for which the data is being processed and the individuals or organisations to whom the data may have been disclosed.

- To be given a copy of the data in an intelligible form, with any unintelligible terms explained.

- To be provided with any information available to LSST about the source of the data.

- To be given an explanation as to how any automated decisions taken about them have been made if a student specifically requests it. These rights apply to electronic data, and to data in "manual" (i.e. non-electronic) formats, subject to certain limitations in regard to unstructured manual data (see below).

- Further information about rights under the Data Protection Act is available on the website of the Information Commissioner (www.ico.gov.uk).

What are the exemptions?

The Data Protection Act includes various exemptions which specify the circumstances in which an organisation can refuse to provide access to personal data. The most likely situations in which LSST could lawfully refuse a SAR are where:

- The release of the data would jeopardise the prevention or detection of crime or the apprehension or prosecution of offenders.

- You have requested access to an examination script, other than examiners' comments.

- You have requested data contained in a confidential reference provided by LSST.

- The data is covered by legal professional privilege.

If LSST withholds data as a result of an exemption under the Data Protection Act, LSST will explain why the data has been withheld and cite the relevant exemption, unless doing so would itself disclose information which would be subject to the exemption.

The Data Protection Act allows LSST to refuse to provide data if the effort in doing so would be disproportionate, or if the same or similar data has already been provided to the person requesting it or their associates and a reasonable interval has not elapsed since the previous SAR. In addition, if LSST reasonably requires further information from the person requesting the data in order to locate the requested data and LSST has informed the person requesting the data or their representatives of this, LSST is not required to comply with the SAR until the person requesting the data or their representative supplies LSST with further information.

LSST has to protect the Data Protection rights and other legal rights of other individuals when responding to SARs. Information which does not relate to a student may be 'blanked out' or edited out, particularly if it relates to other individuals. Sometimes LSST may not be able to release data relating to students or their representatives because doing so would also reveal information about other persons who have not consented to their data being released and it would not be reasonable in the circumstances to release the data without their consent. In such cases, the student or their representatives will be informed that data about the student has been withheld and the reasons for doing so.

What happens after the SAR is received?

LSST will send an acknowledgement of the request as soon as possible. This will indicate the deadline by when LSST will send a response. LSST may also ask to provide further information or clarification if LSST requires it to process the request. After LSST receives the SAR, LSST must consider it and respond to it. LSST will respond as soon as possible, and in all cases within 1 calendar month of receipt of the request.

If LSST reasonably requires further information to locate the data which has been requested, LSST will inform you as soon as possible, and the 30 day deadline will commence from the date when LSST receives the further information. LSST will normally send the data electronically through a shared OneDrive folder, unless LSST agrees with the student or their representatives that the data can be supplied in a different format.

The data may take the form of photocopies, printouts, transcripts or extracts, or a combination of these, depending on what is most appropriate in the circumstances. Although students do not have the right to inspect original documents, LSST may offer this to the student or their representatives where supplying copies of the data would involve a disproportionate effort.

If LSST holds no data about a student, the student or their representatives will be informed of this. The student or their representatives will also be informed of any cases where data about the student has been withheld and the reasons for this, including the relevant exemptions (see above), unless doing so would itself reveal information which would be subject to an exemption.

Can I appeal?

You can ask for an internal review if LSST refuses your SAR or you are dissatisfied with the handling of the SAR. Appeals should be sent in writing to the CEO, at the following address:

Chief Executive Officer

London School of Science & Technology
1st Floor Memo House
Kendal Ave
Park Royal
London
W3 0XA

Email: ceo@lsst.ac

The CEO will acknowledge the receipt of the appeal within seven working days and will consult with the LSST Data Protection Officer. A response will be sent to you within 28 calendar days of the receipt of the appeal. If it includes a decision that data should be released, the information will be provided as soon as possible. Students or their representatives can also ask the Information Commissioner for an assessment as to whether LSST has processed data in accordance with the Data Protection Act. The Commissioner can be contacted at the following address:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom

Telephone: 0303 123 1113
Fax: 01625 524510

APPENDIX B: LSST DATA BREACH REPORTING FORM

(For use by staff or students to report suspected or actual breaches of student data)

1. Reporter Details

Name:

Role: ☐ Staff ☐ Student

Department / Campus:

Email Address:

Phone Number:

2. Date and Time of Incident

Date incident occurred or was discovered:

Approximate time (if known):

3. Description of the Incident

(Please provide a clear, factual summary of what happened. Include how the breach was discovered and any actions taken so far.)

4. Type of Data Involved

(Tick all that apply)

☐ Full names
☐ Student ID numbers
☐ Contact information (email, phone, address)
☐ Passport or visa data
☐ Attendance records
☐ Academic performance or results
☐ Special category data (e.g., health, ethnicity)
☐ Financial data
☐ DBS or criminal offence data
☐ Other: _____

5. Number of Individuals Affected (if known)

Approximate number of individuals affected:

Names of affected students (if known/applicable):

6. How Was the Data Shared or Compromised?

(Tick all that apply)

☐ Sent to the wrong recipient (email)
☐ Shared with unauthorised internal staff
☐ Forwarded without authorisation
☐ Lost/stolen device or USB
☐ Data uploaded to incorrect location
☐ View-only restrictions bypassed
☐ Downloaded to a personal device
☐ Other: _____

7. Actions Taken So Far

(Include who was notified, what steps were taken to contain the breach, and whether access was removed or restricted.)

8. Are Any External Parties Involved or Affected?

☐ Yes ☐ No

If yes, please describe:

9. Declaration

I confirm that the information provided is accurate to the best of my knowledge. I understand that the LSST Data Protection Officer and IT Department may contact me for further details and investigation.

Signature (if submitting by email, type your full name):

Date:

10. Submission Instructions

Please submit this completed form to:

Noman.Nafees@lsst.ac (LSST Data Protection Officer)
CC: registry@lsst.ac and it@lsst.ac

Subject line: URGENT: Data Breach Report - [Your Name or Department]

VERSION HISTORY

Version	**1.0 – 3.1**	
Original author(s):	Data Protection Officer Legal Advisor	
Reviewed by:	Executive Committee	September 2016 September 2017 May 2018 September 2018
Version	**3.2**	
Revised by:	Quality Audit Manager Legal Advisor	
Revision summary:	*Factual updates: Change of data protection officer; Document formatting and version control applied. Changes Reviewed by the Publications Committee.*	
Approved by:	Legal Advisor / Executive Committee	May 2020
Version	**3.3**	
Revised by:	Quality Audit Manager Legal Advisor Head of Registry	
Revision summary:	*Annual review and update. Addition of clause in recording lectures. Expanded definition of personal data. Addition of SAR form template*	
Approved by:	Board of Governors	October 2020
Version	**3.4**	
Revised by:	Quality Unit Legal Counsel Head of Registry	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	October 2021
Version	**3.5**	
Revised by:	Head of Registry General Counsel	
Revision summary:	*Annual review and update. Minor grammatical changes.*	
Approved by:	Board of Governors	November 2022
Version	**3.6**	
Revised by:	Senior Human Resources Manager IT Department	
Revision summary:	*Document owner changed.*	
Approved by:	Board of Governors	March 2023
Version	**4**	
Revised by:	Senior Human Resources Manager IT Department	
Revision summary:	*Document owner changed.*	

Approved by:	Board of Governors	March 2023
Version	**5**	
Revised by:	Quality Unit	
Revision summary:	Section 1.5 added on processes following a data breach, GDPR rights under Section 2 broken down into more detail, Section 2.2 added on students' ability to exercise their GDPR rights and how. Section 9.1 amended to reflect updated information on Retention of Records, section 9.2 added to show a table of retention. Minor grammatical corrections, document format applied, version control applied.	
Approved by:	Board of Governors	March 2025
Version	**6.0**	
Original author(s):	Data Protection Officer Legal Advisor	
Revised by:	Assistant Registrar Quality Unit	
Revision summary:	*Telephone number, email address, IP address, and username added under point 1.3. UK GDPR and Data Protection Act 2018 referenced throughout document to reflect updated legislation. Point 1.5. added on ethical standards in data handling. Point 2.1. added on the process of exercising data rights. EU changed to UK throughout document. Point 9.1. updated to include process following the end of retention periods. Section 10 added on reporting and managing data breaches. Section 12 added on third party access to student data. Section 13 added on student consent and opt-out options. New data breach reporting form added under Appendix B. Minor grammatical corrections, document format applied, version control applied.*	
Reviewed by:	Publications Committee	February 2026
Approved by:	Board of Governors	February 2026
Version	**7.0**	
Original author(s):	Data Protection Officer Legal Advisor	
Revised by:	Assistant Registrar Quality Unit	
Revision summary:	**Annual review and update -** External DPO contact details changed from Bulletproof to Worknest. Minor grammatical corrections, version control applied.	
Reviewed by:	Publications Committee	October 2026
Approved by:	Board of Governors	October 2026