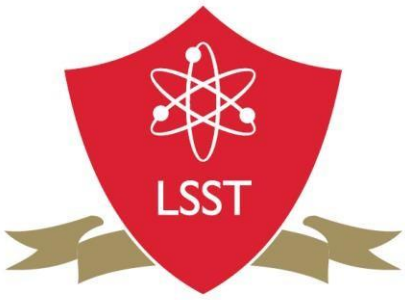


LONDON SCHOOL
OF SCIENCE & TECHNOLOGY

Employee Data Protection and Records Management Policy

Version 8.0

Approved by the Board of Governors

Last Amendment: August 2026

DOCUMENT INFORMATION

Document owner(s)*: Senior Human Resources Manager and IT Department

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 2
1. POLICY STATEMENT 4
1.5. Definitions 4
2. THE DATA PROTECTION ACT (2018) AND GDPR 5
3. PRIVACY NOTICES – HOW STAFF AND STUDENT DATA IS HANDLED 6
3.3. Employee Privacy Notice 6
3.4. Automated Decision Making 9
3.5. Your Rights 9
3.6. Requests for Access to Personal Data (Subject Access Requests – SARs): 10
3.7. Responsibilities and Good Practice 11
3.8. Contact Details for Data Protection 11
4. EMPLOYEE RECORDS MANAGEMENT 12
4.3. Types of Employee Records 13
4.4. Records Management: Good Practice 13
5. REPORTING AND MANAGING SUSPECTED DATA BREACHES 14
5.1. Purpose 14
5.2. Definition of a Data Breach 14
5.3. Staff Responsibilities 15
5.4. Reporting a Suspected Breach 15
5.5. Investigation and Response 16
5.6. Document Sharing and Access Protocol 16
5.7. Non-Compliance and Disciplinary Action 16
5.8. Related Policies and Documents 17
APPENDIX A: SUBJECT ACCESS REQUEST FORM 18
APPENDIX B: GUIDANCE FOR PROCESSING EMPLOYEE RECORDS SECURELY 23

VERSION HISTORY 28

1. POLICY STATEMENT

1.1. All London School of Science and Technology (LSST) employees are expected to abide by this Employee Data Protection & Records Management policy.

1.2. The LSST is registered with the Information Commissioner's Office (ICO) as a data controller.

1.3. All personal data will be gathered, held and processed in accordance with relevant legislation (including the Data Protection Act 2018), good practice guidance (including from the Information Commissioners Office and CIPD) and other relevant professional and ethical codes of conduct.

1.4. Deliberate abuse of the Data Protection principles by members of staff will be treated as gross misconduct and disciplinary action will be taken.

1.5. Definitions

1.5.1. "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.

1.5.2. Examples of Personal Data include:

- Name, home and work addresses.
- Telephone number and email addresses.
- 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.
- Nationality, racial/ethnic origin.
- Education history including qualification details.
- Images caught on close circuit television (CCTV).

1.5.3. “Data controller": a data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

1.5.4. “Staff”, “students” and “other data subjects”: may include past, present and potential members of those groups.

1.5.5. “Other data subjects” and “third parties”: may include contractors, suppliers, contacts, referees, friends or family members.

1.5.6. “Processing”: refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

2. THE DATA PROTECTION ACT (2018) AND GDPR

2.1. Data Protection provides a safeguard for personal privacy in relation to computerised or other systematically filed information. The Data Protection Act 2018 (DPA) implements the EU General Data Protection Regulation (GDPR) into UK law and regulates the use of personal data, meaning information about identifiable, living human beings.

2.2. The principles of the GDPR are:

i. **Lawfulness, fairness and transparency:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

ii. **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Processing for archiving purposes in the public interest or for scientific, historical research and statistical purposes shall not be considered to be incompatible with the initial purpose.

iii. **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

iv. **Accuracy:** Personal data is accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is

inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

v. **Storage limitation:** Personal data that is processed for a specific purpose or purposes shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods as long as the personal data is processed solely for archiving, in the public interest, scientific or historical research or for statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

vi. **Integrity and confidentiality:** Personal data shall 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.

2.3. Sensitive personal data of employees includes ethnic origin, health, trade union membership, sexual life and religious or political beliefs. There are stricter rules on the use of this data and in general it can only be collected and processed with the individuals' explicit consent. Advice should be sought from the HR Department and the Data Protection Officer on the gathering, storage and processing of sensitive personal data.

3. PRIVACY NOTICES – HOW STAFF AND STUDENT DATA IS HANDLED

3.1. Student personal data is processed by LSST in accordance with its student Privacy Notice and Data Protection Policy (Students).

3.2. Staff personal data is processed in accordance with the Employee Privacy Notice, which also sets out staff rights in respect of their personal data.

3.3. Employee Privacy Notice

3.3.1. The School may use and process personal data (both manually and electronically) including Special Category and criminal offence data or information regarding you whilst you are a staff member of the School and after you have left the School. Special Category data includes information held by the School regarding your physical or mental health or condition, your date of birth, nationality, racial/ ethnic origin, sexual orientation/ sex-life, status/marital status, 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). Full information is detailed in the Employee Privacy Notice.

3.3.2. The processing of your personal data for the below purposes is required for the performance of the contract between you and the School, for the School to meet its regulatory obligations to the OfS and statutory requirements in respect of tax compliance, right to work immigration status, pensions, health and safety, as well as the School's legitimate interests including quality assurance and ensuring the 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). You have the right to withdraw such consent at any time.

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

- Identifying data e.g., usernames, names, National Insurance number.
- Tracking data e.g., contact details, computer or BYOD data, location data from the online timesheet system.
- Medical and health data e.g., sick notes, details of disability and reasonable adjustments.
- Career history data e.g., employer or past academic references, qualification history.
- Criminal records e.g., enhanced DBS checks for roles involving supervising working with vulnerable adults.

3.3.4. The purposes for which the School may process your personal data (including Special Category Data) include:

- The administration of your employment (including payment of salary, PAYE reporting, and making statutory deductions).
- DBS checking where required for a role involving children or vulnerable adults.
- The provision of the School's services and facilities to you and the protection of your health, safety and welfare whilst at the School.
- The issue and operation of the School's ID card in accordance with the employee or contractor handbook.
- Equal opportunities monitoring.
- The provision of references about you.
- The provision of information to any regulator, government body or agency.
- For safety purposes.

- For enrolment into the company pension scheme and making pension contributions and deductions.
- For enrolment onto the company health provider scheme.
- For establishing, exercising or defending legal rights (including Employment Tribunals and external legal advisers).
- For enrolment onto training courses.
- Quality assurance of any course you are involved in delivering.
- Occupational health, attendance and performance monitoring.

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

3.3.6. 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, such as policies, information security, staff training and procedures to ensure your information is protected. The recipients of your data will be employees and contractor or consultant staff of LSST (e.g., security contractors, consultant finance officers), future employers who ask for references and, where required, public authorities such as UKVI, regulatory and quality assurance agencies such as the OfS. We may also share certain personal data with our insurers and professional advisors e.g., where required to defend a legal claim.

3.3.7. In some circumstances your personal data will be processed by a third party on our behalf – e.g., a recruitment agency, or contractor finance and 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.

3.3.8. The School collects, processes and stores criminal offence data about past convictions, including enhanced DBS check reports, details of unspent convictions and DBS certificates. This is required for the performance of your contract of employment where you are involved in supervision of students working with children or vulnerable adults on Health & Social Care courses, or where your role involves routine work with vulnerable adults (e.g., a Safeguarding Officer), and otherwise for the legitimate interest of protecting the safety of staff and students of the School. We do not keep a comprehensive record of criminal offence data.

3.3.9. In some circumstances, the School may wish to use data in the form of photographs, or video or audio recordings, of classroom settings as part of general marketing

materials for example in the School'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.

3.3.10. Job application data will be retained for 6 months from the date of the application if a job application is not successful. All other personal data, including successful applicant's application data, will be retained only for as long as necessary where required by statutory retention periods and for no longer than 7 years from the end of your employment with the School in all other cases.

3.4. Automated Decision Making

3.4.1. We and our data processors may make such decisions about you without human involvement. This may include profiling. The main instance in which this occurs is automatic rejection of candidates applying through third-party online recruitment systems if you do not meet the relevant attributes (e.g., a language or driving licence requirement), qualifications or grades required for a role. This is necessary for entry into your employment or service contract with the School and is monitored regularly to ensure it works correctly. If you think an automated decision has led to your rejection in error, you may raise a complaint by sending an email to hr@lsst.ac or to the Data Protection Officer.

3.5. Your Rights

3.5.1. The School's processing of your personal data is subject to your rights under the GDPR: (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) i.e.:

- The right to access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The right to be informed.

3.5.2. Further details are available in the Employee Privacy Notice.

3.5.3. If the School does not process your data fairly, you have the right to lodge a complaint with the UK data protection supervisory authority – the Information Commissioners Office (ICO): https://ico.org.uk/concerns/handling/ within 3 months of

your last contact concerning the matter with the School (or such other time limit as the ICO may specify).

3.6. Requests for Access to Personal Data (Subject Access Requests – SARs):

3.6.1. People whose data is kept (data subjects) have the right to be informed whether data about them is held and the purpose for which the data is used and to obtain a copy of the data – this can be done by making a SAR (Appendix A). This right now applies to most types of information held about an individual in electronic or paper form, subject to certain exemptions. Data Protection requests can be submitted in any clear and unequivocal means and may require proof of ID. A response must be sent within 1 calendar month of the request.

3.6.2. SARs from employees or contractors should be directed to the HR department (hr@lsst.ac). Requests from students should be directed to the Registry (registry@lsst.ac). On receipt of a SAR, the HR Department or Registry will log the request before forwarding it to the IT Department for processing. The IT Department will copy the request to the School's appointed Data Protection Officer as soon as possible.

Persons making a SAR can, if they wish, use the form in Appendix A.

3.6.3. The procedural steps for handling SARs are as follows:

- Upon receipt of a Subject Access Request from the HR department or Registry, the IT Department will send an email to the requestor acknowledging receipt of the SAR and ensure a response is sent within 28 days from the date when the SAR was first received.

- The IT Department will verify that the requestor is the data subject or authorised to act on the data subject's behalf.

- The IT Department will work with relevant departments to gather all personal data requested by the requestor and depending on the nature of the request he/ she may:

    - Place copies of all requested personal data on a shared OneDrive and securely send the requested information to the requester by email or post if the data only exists in hard copy documents, or

    - Lock access to (or seal in an envelope if hard copy) the personal data and immediately forward a request to the DPO for confirmation that the data can be erased, then delete and destroy all copies of the data, or

    - Verify the inaccuracy of the data and accuracy of new data provided and make any necessary corrections.

- In the case of a complaint being received, rectify if possible or forward to the responsible line manager, copying the complaint by email to the DPO.

- The IT Department will send an email to the requestor telling them what action is being taken and when they can expect to receive a response from LSST.

3.7. Responsibilities and Good Practice

3.7.1. If you are a staff member responsible for the collection of personal data (either as a manager or supervisor or as an individual) then:

- Be sure that data subjects have been informed about how the information will be used and who it will be shared with, by showing or providing them a copy of the LSST Privacy Notice.

- Where you need to seek their consent for the collection or use of their data e.g., for participation in promotional photographs or marketing materials, make sure you obtain express and clear written consent and give the data subject a clear means to withdraw that consent.

- Take measures to ensure personal data is up to date, accurate, appropriate and secure. Electronic files should be password protected and access to computers or databases containing personal data should be password protected and timed. Hardcopy files should be kept in secure and lockable cabinets or draws and in lockable rooms. Personal data should not be left out on desks unattended.

- Consider Data Protection before releasing data to third parties, especially those outside LSST. Remember that the family and friends of students and staff have no automatic right to data about them nor do the police and the government, unless certain conditions are met. If in doubt about whether to release personal data, contact HR, Registry or the Data Protection Officer.

- Do not keep personal data for longer than is necessary and always dispose of personal data securely and thoroughly.

- Remember that people have the right to ask about data held about them. Requests for personal data should be referred to the IT Department for staff members and to Registry for students. Guidance on the procedure for making requests is contained in Appendix A.

3.8. Contact Details for Data Protection

- **<u>London School of Science and Technology Ltd (Data Controller)</u>**

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

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

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

  registry@lsst.ac

- **Human Resources (for non-student Subject Access Requests)**

  hr@lsst.ac

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

  20 Grosvenor Place, London SW1X 7HN

  DPOsupport@worknest.com

4. EMPLOYEE RECORDS MANAGEMENT

4.1. Employee Records management is about ensuring that the information that we need to document what we do is generated and kept as efficiently as possible. Records act as evidence of our decisions and activities and preserve information which we may need in the future. Employees' records are kept in paper form as well as electronically. The law requires us to manage the records we keep effectively in order to meet Data Protection requirements and so that we can produce information when it is requested under the Freedom of Information Act and other laws. Having good records management also helps us to work better.

4.2. Employees Records management helps LSST organise its records in a consistent and coherent way, saving time when looking for information.

- Paper records are maintained and a process of keeping the records in electronic form runs parallel to save space (both physical storage space and server space). Records are kept for no longer than necessary. Records are disposed of according to agreed procedures.

- Our records have value as evidence and are used to defend our and others' legal rights when necessary. Records are kept in ways which ensure that their authenticity cannot be challenged, e.g., in a court of law.

- LSST ensures it complies with legal, regulatory and contractual requirements. Good records management is not only necessary for Freedom of Information and Data Protection reasons. Regulatory frameworks like the Office for Students (OfS) may require LSST to keep records and LSST also needs to keep records to show compliance with contracts and for audit purposes.

4.3. Types of Employee Records

- **Active records:** are records that are needed for frequent processing or reference by the creating department. Active records are the responsibility of the creating office, unit or department. They must be filed and stored appropriately within meaningful record systems.

- **Reference records:** are records which are no longer processed or used regularly, but which need to be retained for a fixed period for reference, administrative or legal reasons. Reference records are the responsibility of the creating office, unit or department. They must be filed and stored appropriately within meaningful record systems. These will usually be kept for a period of 7 years from the date they cease to be active after which period they are disposed of.

- **Disposal:** records must be disposed of once their life has expired. Records must be disposed of according to agreed retention schedules. Records must be disposed of in a manner appropriate to their confidentiality or sensitivity. Records that are no longer needed must be disposed of or transferred to the Archives.

- **Archive:** Records of long-term historical or evidential value must be transferred to the Archive and not stored in offices. Once records have been transferred to the Archive they cannot be recalled by faculty, units or departments for further filing or processing. They will be made available for reference.

- **Retention schedules.** These specify how long you should keep common types of records. A model classification scheme and retention schedule for higher education has been developed by the Joint Information Systems Committee (JISC), which is the recommended good practice for the sector and should be used as the default retention schedule across LSST.

4.4. Records Management: Good Practice

- Use appropriate and professional language, particularly when referring to individuals. Ensure what is to be released fulfils the criteria under Data Protection or Freedom of Information.

- Remember that records are owned by LSST. If an employee leaves LSST they are no longer entitled to access LSST records. The person responsible is to maintain and keep them in an orderly state.

- LSST is in the process of standardisation by:

    - Setting up a classification scheme and retention schedule. LSST's aim is to use the same scheme for your paper and electronic information, so that your records are organised consistently.

- Setting up a naming convention for your electronic files. This will make it easier to identify what a file relates to, without having to open it.

- All working for LSST are assigned an LSST email address in the following format: name.surname@lsst.ac or name@lsst.ac (if requested by the staff member). Emails are records too. Most correspondence now takes place by email and email is used to make key decisions. All relevant emails are saved on the LSST record keeping system, e.g., by printing them out and adding them to personal files of the staff member. Emails can also be saved on the LSST HR folders available on the LSST OneDrive.

- All electronic shared directories have to be placed in LSST HR OneDrive folders whilst shared paper files for information that other colleagues need to access are to be filed in the personal files of staff members. No HR department staff will maintain any documents relating to staff members in their personal possession and no HR staff member can take any document whether in paper or electronic format outside the premises of LSST.

5. REPORTING AND MANAGING SUSPECTED DATA BREACHES

5.1. Purpose

5.1.1. This section outlines LSST's policy and procedures for reporting, assessing, and responding to suspected or actual breaches of staff/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.

5.2. Definition of a Data Breach

5.2.1. 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."

5.2.2. Examples include but are not limited to:

- Sending staff/student data to the wrong recipient.
- Documents containing staff/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.

5.3. Staff Responsibilities

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

- Ensure that staff/student data is shared only with authorised individuals with a legitimate academic or administrative need.
- Never download or forward staff/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.

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

5.4. Reporting a Suspected Breach

5.4.1. 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 data document).
    2. **Report the breach to the Data Protection Officer (DPO):**
       Email: DPOsupport@worknest.com (WorkNest Limited)
       CC: **registry@lsst.ac** and **it@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.

5.5. Investigation and Response

5.5.1. 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.

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

5.6. Document Sharing and Access Protocol

5.6.1. To prevent inappropriate sharing:

- Student/staff 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.

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

5.7. Non-Compliance and Disciplinary Action

5.7.1. 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.

5.8. Related Policies and Documents

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

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 by General Data Protection Regulations.

Please complete the table below and return the form by post to the 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 verify that you are the person named above. We may ask for one of the following documents – Please tick the ones you are supplying:

- ☐ A copy of your passport
- ☐ A copy of your photocard driving licence
- ☐ A copy of an 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 a right of access to the personal data which 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 SARs and how to complain if you are dissatisfied.

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

- To be given a description of the data, the purpose for which the data is being processed and those to whom the data is 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, and
- If a staff member specifically requests it, to be given an explanation as to how any automated decisions taken about them have been made. These rights apply to electronic data and to data in "manual" (i.e., non-electronic) formats, subject to certain limitations with regard to unstructured manual data (see below).
- Further information about staff 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 the examiners' comments.
- You have requested data contained in a confidential reference provided by LSST.
- A staff member has requested data which record LSST's intentions in relation to any negotiations with that staff member and the release of the data would prejudice those negotiations.
- The data is covered by legal professional privilege.

If LSST withholds data from a staff member or anyone as a result of an exemption under the Data Protection Act, LSST will explain why the data has been withheld and 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 staff member 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 the data or their associates and a reasonable interval has not elapsed since the previous SAR. In addition, if LSST reasonably requires further information from a staff member in order to locate the data which the staff member has requested and LSST has informed the staff member or their representatives of this, LSST is not required to comply with the request until the staff member or their representatives supply LSST with the requested 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 staff member may be redacted, particularly if it relates to other individuals. Sometimes LSST may not be able to release data relating to a staff member 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 person requesting the information will be informed that requested data has been withheld and the reasons for doing so.

What happens after a SAR is received?

LSST will send an acknowledgement of the SAR as soon as possible. This will indicate the deadline by when LSST will send a response. LSST may also ask the person submitting the SAR to provide further information or clarification if LSST requires it to process the SAR. After the 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 SAR.

If LSST reasonably requires further information, LSST will inform you as soon as possible. In this case, the 30-day deadline will commence from the date we receive the further information. LSST will normally send the data electronically through a shared OneDrive folder, unless LSST agrees with the person requesting the information 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 staff members and their representatives do not have the right to inspect original documents, LSST may offer this to a staff member or their representatives where supplying the data would involve disproportionate effort.

If LSST does not hold the requested data the staff member or their representatives will be informed of this. They will also be informed of any cases where data about them has been withheld and the reasons for this, including the relevant exemptions (see above), unless doing so would itself reveal the information that is the 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:

F.A.O Chief Executive Officer

London School of Science & Technology
1st Floor Memo House
Kendal Ave,
Park Royal,
London
W3 0XA
mailto:ceo@lsst.ac
Email: ceo@lsst.ac

The CEO will acknowledge the appeal within seven working days, and will consult with the Data Protection Officer. A response will be sent to you within 28 calendar days of receipt of the appeal. If it includes a decision that data should be released, the information will be provided as soon as possible. Staff 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

https://ico.org.uk/make-a-complaint/data-protection-complaints/

APPENDIX B: GUIDANCE FOR PROCESSING EMPLOYEE RECORDS SECURELY

Security must be appropriate to the nature of the data to be protected. In research data will almost inevitably include "sensitive" information, which requires the highest level of security and confidentiality. The required levels of security must be maintained throughout processing at LSST, at the premises where data processors are located, at home, on laptops, etc.

If the project involves a group of personnel, one member should be responsible for overall data security and should control who has data access, for how long and at what level. This could be an administrator who need not necessarily have full access himself/ herself. Where data processing is delegated by the data holder to others (e.g., for scanning, transcription, or statistical analysis) the data holder must ensure that all data processors, including temporary employees, or staff who have been asked to undertake work in their own time, are required to sign a standard form, relating to compliance with confidentiality and security requirements.

Recommended security measures:

- There should be a suitable lock on the door to a research unit.
- Manual data should be stored in a locked facility when not under the direct supervision of a data holder or processor. Manual data includes:
    - Questionnaires.
    - Notes and other paper files.
    - Audio and videotapes.
    - Photographs and negatives.
    - Removal digital media (e.g., memory sticks, CD/DVD ROMs, external hard drives).

Access to data stored on a computer should be controlled by passwords and, where appropriate, access to individual files should also be password-protected. Passwords should be known only to authorised people and changed at regular intervals. Password protection may not be enough to keep data safe from hackers and data encryption should be considered where possible.

Do not leave a PC unattended with an active, password-protected program still running. Back up research data regularly. Back up files should be kept on a secure shared drive, rather than removable digital media (for help in accessing such a drive, consult your IT technician). When working at home or on a laptop, the opposite is true: personal data should be kept on password-protected media and not on the hard drive of a home PC or a laptop.

Removable digital media (e.g., memory sticks, CD/DVD ROMs, external hard drives) must not be used unless the data on them is password-protected and has been backed up to OneDrive. Removable media must be disposed of securely by IT. Keep in mind the potential damage to individuals which may result if a disk is lost or stolen.

When staff work at home, security should be of the same standard as that which is provided at LSST premises. Consider the following:

- Access of other individuals (e.g., family members) to the PC, to other automated data (e.g., digital images) or to paper files.
- Protection against theft or loss (of the PC, disks, memory sticks, tapes, digital cameras, laptops, mobile telephones).
- Back-up provisions.

Consider the security of data 'on the move' e.g., e-mail, posting work to a co-researcher, using a laptop, etc. If possible, use or initiate 'safe-haven' procedures for such communications e.g., locate the fax machine or printer in a lockable room with restricted access. If no 'safe-haven' is available, omit identifying data from the fax, provide numbers instead and then telephone with the 'missing' data. In the case of e-mail, send personal information in an attachment which has been password-protected and communicate the password by telephone or by separate email.

Email should not be used for confidential or "sensitive" data (unless encryption is used).

Retention & Disposal

Personal data must be disposed of securely:

- Printed material should be shredded and/ or burnt.
- Tapes and disks must be completely cleaned before re-use.
- Computers must be completely cleared of data before disposal or use for other purposes (this procedure also applies when a LSST laptop is being borrowed).
- Any breaches of security must be investigated and remedied.

NB: Simply deleting files from a computer, laptop or removal digital media is not sufficient to remove data completely. Multiple re-formatting is necessary to ensure that data are irretrievable.

Make plans for the storage and disposal of data when a project is finished.

LSST employee record-keeping responsibilities

LSST has a responsibility to ensure that every staff member and casual worker and every migrant visitor, however brief the visit, is properly entitled to work in and/or participate in the activities of LSST.

It is essential that LSST complies with immigration laws and with the policies and regulations of the Home Office.

LSST employees and casual staff may have the right to work in the UK through a range of immigration statuses. These include, among others, British or Irish citizenship, status under the EU Settlement Scheme (pre-settled or settled), permission under a sponsored route such as the Skilled Worker route, Indefinite Leave to Remain (ILR), various unsponsored work routes, dependant visas, student visas (subject to working restrictions), or UK Ancestry visas.

In all cases, LSST is legally required to conduct a compliant Right to Work check before employment or engagement begins and to retain evidence of that check in accordance with Home Office guidance. Acceptable methods include manual document checks, online RTW checks (including for eVisa holders), or checks conducted via an accredited Digital Verification Service where permitted. Evidence must be retained to establish a statutory excuse against civil penalties.

For individuals who are *not* sponsored by LSST (e.g., those holding their own immigration permission such as ILR, EUSS status, dependant visas, or other non-sponsored categories), LSST must still undertake and retain a valid RTW check. Although these individuals do not impose sponsor-specific reporting duties, LSST must ensure they have the appropriate immigration entitlement to undertake the work and be able to demonstrate this to the Home Office if required.

Record-keeping responsibilities for formerly sponsored Skilled Worker (formerly Tier 2) migrants

LSST holds all required information relating to previously sponsored Skilled Worker (formerly Tier 2) migrants within the HR Department and/or with the Authorising Officer.

In accordance with Home Office sponsor-licence compliance requirements, LSST must retain specific documents and records for a minimum of 12 months after it ceases to sponsor a worker, or until a Home Office compliance visit has taken place, whichever is later. These obligations apply when sponsorship ends due to:

- Withdrawal or revocation of LSST's sponsor licence.
- Cessation of the individual's employment, or

- The worker switching into a category not sponsored by LSST (e.g., ILR, dependant visa, or another unsponsored route).

Documents may be digitised for secure storage, provided they remain accessible and can be produced promptly for inspection during a Home Office compliance visit. Original documents may be archived or destroyed once compliant digital copies are held. After documents have been inspected and approved at a compliance visit, LSST may securely dispose of them, unless retention is required for other legal purposes (e.g., RTW evidence, payroll, or employment law requirements).

Please note that certain personnel records—such as Right to Work check evidence and pay-related information—must be retained for longer periods under separate employment and statutory record-keeping rules.

Documents LSST must retain for formerly sponsored Skilled Worker/Tier 2 migrants

1. Identity and right-to-work documents

- Passport or UK immigration status document.
- Biometric Residence Permit or eVisa status evidence showing permission to work in the UK.
- National Insurance number.
- Current UK contact details (address, telephone number, mobile number).
- Historic contact details maintained throughout employment.

2. Employment and HR documents

- Absence record covering the period of sponsorship.
- Contract of employment or contract for services, clearly stating:
    - The names and signatures of all parties.
    - Contract start and end dates.
    - Job title and description of duties.
    - Salary details.

- Skills, qualifications and experience required for the role.

3. Resident Labour Market Test (RLMT) evidence (where applicable)

For roles that required RLMT under the rules in force at the time of recruitment:

Where the vacancy was advertised online, LSST must retain a printout or screenshot taken **on the date the advert first appeared**, which clearly shows:

- Name of the website.
- Full content of the advert.
- Date of printing/screenshot.
- URL.
- Closing date for applications.

Where the role was exempt from RLMT, LSST must retain a note confirming the applicable exemption (e.g., shortage occupation role, recent graduate recruitment, or other exemption permitted at the time).

VERSION HISTORY

Version	**1.0-4.0**	
Original author(s):	Head of Operations Head of Security	
Reviewed by:	Executive Committee	September 2016 September 2017 September 2018 September 2019
Version	**4.1**	
Revised by:	Quality Audit Manager Head of Legal Services	
Revision summary:	*Annual review and update. Change of DPO details. Document reformatted.*	
Approved by:	Board of Governors	October 2020
Version	**4.2**	
Revised by:	Senior Human Resources Manager General Counsel	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	November 2022
Version	**4.3**	
Revised by:	Senior Human Resources Manager IT Department	
Revision summary:	*Document owner changed.*	
Approved by:	Board of Governors	March 2023
Version	**5**	
Revised by:	Senior Human Resources Manager IT Department	
Revision summary:	*Annual review and version control applied.*	
Approved by:	Board of Governors	October 2023
Version	**6**	
Revised by:	Quality Unit	
Revision summary:	*Bulletproof contact email changed, FAX number replaced with website link, minor grammatical corrections, document format applied, version control applied.*	
Approved by:	Board of Governors	March 2025
Version	**7.0**	
Original author(s): Revised by:	Head of Operations Head of Security HR Quality Unit	
Revision summary:	*UK GDPR and Data Protection Act 2018 referenced throughout document to reflect updated legislation. Additional examples of personal data added under point 1.5.2. Additional special category data examples added under point 3.3.1, reference to Employee Privacy Notice. Additional reasons for the School processing personal data added under 3.3.4. EU changed to UK throughout*	

	document. Further information added under Appendix B, LSST Employee Record-Keeping Responsibilities. Addition of Section 5 on reporting and managing suspected data breaches. Minor grammatical corrections, document format applied, version control applied.	
Reviewed by: Approved by:	Publications Committee Board of Governors	February 2026 February 2026
Version	**8.0**	
Original author(s): Revised by:	Head of Operations Head of Security HR 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: Approved by:	Publications Committee Board of Governors	October 2026 October 2026