Data and Information

4.1 Data Protection Policy

Introduction

Data protection legislation regulates "the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information" by data controllers, such as the London Interdisciplinary School. It requires the School to process, use and store the personal data relating to potential staff and students current staff and students, former staff and students, contractors, website users and contacts ("data subjects") in a way that is fair, proportionate, secure and justified. Data protection legislation changed on 25th May 2018, when the General Data Protection Regulation (GDPR) came into force, replacing the existing Data Protection Act 1998.

This Policy describes the responsibilities of the School, its staff and students in complying fully with the provisions of GDPR and the associated data protection legislation, and in adhering to the six principles of Data Protection. In doing so, this policy seeks to:

- Clarify how personal data must be processed, and the School's expectations for all those who process personal data on its behalf;
- Ensure that the School complies with data protection law and good practice;
- Protect the School's reputation, by ensuring that the personal data entrusted to the School is processed in accordance with the rights of data subjects;
- Protect the school from risks of personal data breaches and other breaches of data protection law.

Any breach of this Policy may lead to disciplinary proceedings.

Scope

The execution of this Policy applies to all staff of the School. This Policy relates to all personal data held by the School on:

- Students (including current students, former students, applicants and alumni)
- Employees (including employees past and present, job applicants, contractors, board members, volunteers, consultants, independent examiners and invigilators)
- Visitors (including prospective applicants (e.g. enquirers), prospectus requesters, event registrants and attendees, external speakers, and all other individuals who have expressed an interest in: studying at LIS; participating in its activities in another way, such as one of LIS' outreach programmes; and one off events, e.g. Discovery Days. Also includes agents, third parties and partners, as well as employers offering internships through the School).

This Policy applies to all personal data processed or controlled by the London Interdisciplinary School, regardless of the location of where the data is held, the ownership of the equipment used, who created the data, and the data subject.

Definitions

The following definitions are used in the General Data Protection Regulation, and are referenced in this policy:

Personal Data are data that can identify living individuals. This may include names, contact details, images, or numerical or statistical information from which an individual's identity can be derived.

Special Category Data are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation.

The **Data Subject** is the individual who is the subject of personal data.

The **Data Controller** determines the purposes for which personal data are processed. The controller is ultimately responsible for the personal data, whether they pass the data to a data processor or not. This includes the responsibilities of responding to access requests and complaints from data subjects.
A **Data Processor** is any individual or organisation that processes personal data on behalf of, and according to the purposes defined by, the data controller.
Consent is an agreement, which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes, by which they, by a statement or clear positive action, signify agreement to the processing of their personal data.
Profiling is any form of automated processing of personal data where the personal data is used to evaluate certain personal characteristics relating to an individual, in particular to analyse aspects concerning that individual's performance at work or School, economic situation, personal preferences or interests, health, reliability, behaviour, location or movements.
Processing is any activity that involves the use of personal data, including obtaining, recording, holding the data, or carrying out any operation on that data, including organising, amending, retrieving, using, disclosing, erasing, destroying the data, or transferring it to third parties.

Principles

The GDPR sets out six data protection principles. The School is required to follow these principles in the processing of any personal data.

Lawfulness, Fairness and Transparency: The School will explain to its staff, students and any other relevant third parties how and for what purpose it is processing personal data, at the point of collection.

Purpose Limitation: The School will only use the personal data it has for the purposes for which it was collected.

Data Minimisation: The School will only collect personal data that is relevant to the purposes for which it is required.

Accuracy: The School will ensure that data is accurate and up-to-date, and will rectify any mistakes quickly.

Storage Limitation: The School will not retain personal data for longer than is necessary.

Integrity and Confidentiality: The School will protect its personal data against unauthorised access, loss or destruction.

Policies

The School's Accountability

The School must implement appropriate technical and organisational measures in an effective manner to ensure that it is compliant with the six data protection principles. In addition to complying with these principles, the School must be able to demonstrate its compliance.
The School must therefore use adequate resources and controls to ensure and document compliance with the GDPR. This will include:

- Appointing a suitably qualified Data Protection Officer (DPO);
- Implementing privacy by design and default in new initiatives, projects, systems or initiatives that involve the collection, processing, sharing or storing of personal data;
- Describing, embedding, updating and auditing compliance with a School Data Protection Policy;
- Recording and producing the required documentation in relation to the conduct of this Policy, for example with records of data processing and of personal data breaches;
- Training staff on compliance with data protection law, and making a record of this training;
- Regularly testing, auditing and continuously improving the mechanisms and measures that the School has put in place to protect personal data in line with regulations.
- The School is registered with the Information Commissioner's Office (ICO) (registration number ZA494947)

GDPR Principle 1: Lawfulness, Fairness and Transparency

Legal Basis for Processing Data

Processing personal data must meet at least one of the following conditions if it is to meet the "lawfulness" principle:

- The data subject has given consent;
- The data processing is necessary for the performance of a contract;
- The data processing is necessary due to a legal obligation;
- The data processing is necessary to protect an individual's vital interests;
- The data processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller (in the case of the School, this would cover the retention of student pass lists and transcript information for awards and verification);
- The data processing is necessary for the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (in the case of the School, this would cover activities relating to alumni and the marketing of commercial services).

For special category data, the School is required to have additional legal basis for proceeding, as set out in Article 9 of the GDPR:

- Processing is necessary for the purposes of carrying out the obligations, and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law (examples relevant to the School might include sickness absence);
- Processing relates to personal data which are manifestly made subject by the data subject (examples relevant to the School might include alumni research);
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee (examples relevant to the School might include occupational therapy assessments);
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (examples relevant to the School might include the analysis and reporting of equality and diversity information);
- Processing is necessary to protect an individual's vital interests (for example, in a life or death scenario);
- Processing is necessary for legal claims;
- Processing is necessary for public health.

Consent

A data subject's consent must only be obtained if there is no other legal basis for the processing of their personal data. A data subject signals consent if they clearly indicate agreement to the processing, either by a statement or a positive action. An option to provide consent must be separate and distinct from other information presented to the data subject. Evidence of consent must be retained. Consent is required for electronic marketing and some research purposes.

Data subjects must be able to withdraw their consent with ease and at any time, and their request must be actioned as quickly as possible.

Transparency
Under data protection law, the School is required to provide detailed and specific information to data subjects, depending on whether the information was collected directly from data subjects or from elsewhere. This information must be provided through the appropriate privacy notices; it must be concise, transparent, intelligible, easily accessible, and in clear and plain language.

Where the School collects personal data directly from data subjects, for example in the recruitment and enrolment of students or the recruitment and employment of staff, at the time of collection, the information provided to the data subject must include:

- The School's details;
- The contact details of the School's Data Protection Officer;
- The legal basis of processing;
- Where the legal basis is consent, the right to withdraw;
- Where the legal basis is legitimate interest, the specification of that interest (for example, marketing);
- Where the basis is a statutory or contractual necessity, the consequences for the data subject of not providing the information.

Where personal data is collected indirectly, for example from a publically available source or a third party, the School must also provide information on the categories of personal data, as well as any information on the source, as soon as possible after receiving the data. The School must also verify that the personal data was collected by the third party in compliance with the GDPR.

GDPR Principle 2: Purpose Limitation

Personal data must only be collected for specified, explicit and legitimate purposes. It must not be further processed in any manner that is incompatible with these purposes, unless the data subject has given consent, or there is a lawful exemption from data protection law requirements.

In assessing whether a purpose is compatible with the original purpose, the following factors should be assessed:

- The link between the original purpose for which the personal data was collected, and the intended further processing;
- The context in which the personal data was collected, and whether the data subject would reasonably anticipate the further processing of their personal data, given their relationship with the School;
- The nature of the personal data; specifically whether it involves special categories of personal data, or personal data relating to criminal offences or convictions;
- The consequences of the intended further processing for the data subject;

- The existence of any appropriate safeguards, such as encryption or pseudonymisation.

Provided that prescribed safeguards are implemented (including data minimisation or pseudonymisation), further processing for scientific or historical research purposes will not be regarded as incompatible. This research must not be conducted for the purposes of making decisions about individuals, and it must not be likely to cause substantial damage or distress to an individual.

GDPR Principle 3: Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is being processed. Employees may only process personal data when required to do so in order to perform their job duties. Employees must ensure that when personal data is no longer required for its specified purpose(s), it is deleted or anonymised in accordance with the School's data retention policy and schedule.

GDPR Principle 4: Accuracy

Personal data must be complete, accurate, recorded in the correct files, and kept up to date where relevant. The School must therefore verify the accuracy of any personal data both at the point of collection and at regular intervals going forward. All reasonable must be taken to ensure to amend or destroy inaccurate records promptly.

Where a data subject has requested their personal data to be corrected or erased, the School must inform the recipients of that personal data that this has taken place, where it is reasonable to do so.

GDPR Principle 5: Storage Limitation

Personal data must not be stored in such a way that allows data subjects to be identified for longer than it is needed for the legitimate purposes for which it was collected. Personal data records may be kept for longer than necessary, provided it is anonymised.

Data subjects must be informed of the period for which their personal data is stored in the relevant privacy notice. Employees must take all reasonable steps to securely erase or destroy all personal data that is no longer required given the School's Data Retention Policy and Detailed Data Retention Schedule.

GDPR Principle 6: Security, Integrity and Confidentiality

The School must implement and maintain appropriate safeguards to protect personal data. These safeguards must take into account the potential risks to data subjects as an outcome of unauthorised or unlawful processing, or accidental loss, damage or destruction of their personal data. Safeguards include encryption and pseudonymisation where appropriate and the restriction of access to those who require the data and are authorised to access it. All

employees must handle personal data in such a way that safeguards against unlawful processing and accidental loss, damage and destruction, and that preserves confidentiality.

Data Subject Rights

Data subjects have a number of rights under data protection law. As the data controller, the School must comply with these rights. These are the rights to: information; subject access; rectification; objection; erasure; portability; restriction of processing; and rights in relation to automated decision-making and profiling.

Right to information: The School must adhere to the requirement for fairness and transparency when collecting data from individuals. Specifically, the School must provide data subjects with a Privacy Notice to let them know how, and for what purpose, their personal data are processed. Any data processing must be consistent with that purpose.

Right of access: Data subjects have the right to find out what the School is doing with their data, to check the School is holding it correctly, and to obtain a copy of the data that the School is holding. They have right to know: the purposes for which the data was collected; the categories of personal data being processed; the recipients of the data; retention periods; information about their rights, including their right to complain to the ICO; details of the relevant safeguards where personal data is transferred outside the EEA; and any third-party source of the personal data.

The entitlement is not to documents *per se*, but to such personal data as is contained in the documents. This right of access relates to personal data held electronically and to limited manual records. Personal data must not be disclosed to third parties without proper authorisation; for example, a student's parents do not have an automatic right to access their child's data. It is a personal criminal offence to delete, alter, block or conceal relevant personal data after a subject access request has been received. It should be noted that subject access rules do not apply to examination scripts.

Right to rectification: The School will make every effort to ensure that its data is accurate. Data subjects have the right to require the School to rectify any inaccuracies in personal data being held or processed. In some circumstances, if personal data are incomplete, the data subject can require the data controller to complete the data, or to record a supplementary statement.

Right to objection: Data subjects have the right to object to data processing that is not based on legitimate interests, legal obligation, or is being processed for the purposes of direct marketing or for "scientific or historical research purposes or statistical purposes".

Right to erasure: Data subjects have the right to have their data erased where the data is no longer required for the purpose for which it was originally collected; where the data subject withdraws consent; where the data is being processed unlawfully; or where the data subject has objected to the School's processing for direct marketing purposes.

Right to portability: In limited circumstances, data subjects have the right to receive or ask for their personal data to be transferred to a third party (for example, another university, to which the student is transferring) in a structured, commonly used and machine-readable format.

Right to the restriction of processing: Data subjects have the right to object to specific types of processing, such as processing for direct marketing, research or statistical purposes. The data subject must demonstrate grounds for objecting to the processing relating to their particular situation, except in the case of direct marketing, where the right to object is absolute.

Automated decision-making, including profiling: If the School is making significant decisions about data subjects (including profiling) through purely automated means, such as a computer algorithm, data subjects have the right to either have the decision reviewed by a human being, or not be subject to this kind of decision-making at all.
Exceptions are: where this is necessary for entering into, or performing, a contract with the School; where it is based on the data subject's explicit consent and is subject to safeguards; or where it is authorised by law and is also subject to safeguards.
Requests must be complied with, usually within one month of receipt. Employees at the School who receive any requests to erase, rectify, or restrict processing of personal data should contact the Data Protection Officer.
A charge may be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Privacy By Design and Default

The School is committed to designing privacy into its systems and processes, by implementing appropriate technical and organizational measures (such as pseudonymisation) in an effective manner. The School and its employees must therefore ensure that, *by default*, only personal data that is necessary for each specific purpose is processed. This applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the data; in particular, personal data should only be available to a limited and prescribed number of relevant, authorised persons who need it to discharge their duties.

Data Protection Impact Assessments

Where a new project, process system or initiative is being considered that involves the collection, processing, sharing or storing of personal data, the Department concerned must conduct a Data Protection Impact Assessment. In particular, a Data Protection Impact Assessment must be conducted where new technologies are being introduced (programmes, systems or processes); where automated processing is being introduced, including profiling; where large-scale processing of special category data is being introduced; or where large-scale, systematic monitoring of a publicly accessible area is being introduced. A checklist to be used by Departments to determine whether or not a Data Protection Impact Assessment needs to be carried out in relation to a new project, process or initiative can be found at Annex 4 of this Policy; this checklist is recommended by the ICO.

A template to be used by staff for Data Protection Impact Assessments can be found at Annex 5 of this Policy; this is the template recommended by the ICO.

Conducting Data Protection Impact Assessments at the outset of such new projects, systems or initiatives ensures that issues of data privacy and protection are considered from the design stage. The Data Protection Impact Assessment must: describe the personal data processing, its purposes and the data controller's (i.e., the School's) legitimate interests; identify the degree of compliance of the new process or initiative with data protection regulation; identify risks to data privacy and protection; and set out the measures put in place to minimize or reduce these risks. The Data Protection Officer must be consulted on any DPIA being conducted and their advice sought. Where risks cannot be mitigated, the Data Protection Officer must be consulted. The Data Protection Officer will also monitor ongoing compliance with a DPIA.

Anonymisation and Pseudonymisation: Wherever possible, personal data must be anonymised; or where that is not possible, it must be pseudonymised. This default position supports the protection of personal data.

Data Security

All users of personal data within the School must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally. It is the responsibility of the School's Head of Digital to support compliance against the "integrity and confidentiality" regulatory principle, by ensuring that the appropriate technical measures are in place to protect personal data (in accordance with Article 33 of the GDPR).

Data Protection Incidents

The School is responsible for ensuring appropriate and proportionate security for the personal data it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, alteration, destruction or damage. The School makes every effort to avoid data protection incidents. In the case where such an incident does occur, the following procedure must be followed:

- Any member of the School, including employees and students, who suspects that a data protection incident has occurred, must report it to the School's Data Protection Officer as soon as possible.
- If a reportable breach is deemed to have occurred, the School must notify the ICO as soon as possible, and not later than 72 hours after becoming aware of it.
- Where the breach results in a high risk to the data subject, the data subject must be notified, unless subsequent steps have been taken to ensure that the risk is likely to materialise, or security measures were applied to make the personal data unintelligible (for example, through encryption). Where it would require a disproportionate effort to inform the data subject directly, the School must make a public communication to inform the data subjects affected, so that they can take any mitigating action.

Data Retention

Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted. The School has a Data Retention Policy and Detailed Data Retention Schedule that have been developed in line with legal and business requirements and JISC recommendations.

Data Sharing

When personal data is shared internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, the students in question will need to be provided a new privacy notice.

Where data will be shared with a internships provider to support the School's internships programme, the student will be asked to sign another consent form. The details of this data sharing will be covered in any agreement between the School and the employer.

In the absence of consent, or a legal obligation or other legal basis, personal data should not normally be disclosed to third parties unrelated to the School.

When personal data is shared externally, a legal basis must be determined and a data-sharing agreement between the School and the third-party must be signed. The exception is where disclosure is required by the law, such as certain requests from the Inland Revenue or Department for Work and Pensions, or where the third party requires the data for law enforcement purposes. It should be noted that without a warrant, the police have no automatic right of access to records of personal data. However, voluntary disclosure may be permitted for purposes of preventing or detecting criminal activity, or apprehending offenders. In this case, written assurances should be sought from the police that the relevant exemption applies.

The School may use an external contractor or 'data processor' to store or manage its data. It will process this data only for purposes specified by the School and will be bound by contract to meeting the School's obligations under the General Data Protection Regulation.

Sharing data outside the EU: The GDPR restricts any transfer of personal data to countries outside the EU. Personal data is considered to have crossed borders when it is transferred to a different country, or when it is viewed or accessed in a different country. Personal data may only be transferred outside the EU if one of the following conditions applies:

- The European Commission (EC) has issued a decision confirming that the country to which the personal data is transferred has an adequate level of protection for the data subjects' rights and freedoms;
- Appropriate safeguards are in place (such as binding corporate rules, standard contractual clauses approved by the EC, or an approved code of conduct or certification mechanism);

- The data subject has given explicit consent to the proposed transfer, after they have been notified of any potential risks; or
- The transfer is necessary for one of the other reasons described in the GDPR (including reasons of public interest; to establish, exercise or defend legal claims; or to protect the vital interests of the data subject where they are physically or legally unable to give consent).

Research

Before commencing any research that will involve the collection or processing of personal data, the researcher must give proper consideration to this Policy. They must comply with the fairness, transparency and lawfulness principle, and application of privacy by design and default. This means that wherever possible, personal data used in research must be anonymised or pseudonymised at the earliest possible juncture.

A student should only use personal data for a School-related purpose with the knowledge and express consent of the appropriate member of teaching staff (normally the person responsible for teaching the relevant class or module).

The use of School-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible, data should be anonymised, so that students are not able to identify the subject.

Where a student collects and processes personal data in order to pursue a course of study within the School, and this course of study is not part of a School-led research project, the student is the data controller for the personal data used in the research. Once a thesis containing personal data is submitted for assessment, the School becomes data controller for that personal data. Where a student is processing data whilst working on a School-led research project, the School is the data controller.

Direct Marketing

Direct marketing comprises any communication of material about the sale of products and services to individuals, and the promotion of aims and ideals. For the School, this includes notifications about events, fundraising, and selling our services to applicants, students, alumni and any other potential users. Marketing covers all forms of communication, such as contact by post, fax, telephone, and electronic messaging, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003.

The School must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop. For example, a data subject's prior consent is required for electronic direct marketing (e.g., emails, texts, automated calls). The limited exception for existing customers (e.g., current students), known as the "soft opt-in", allows organisations to send marketing texts or emails if they have obtained the data subject's contact details in the course of a sale to that person; if they are marketing similar services; and if that data

subject has been given the opportunity to opt out of marketing when their details were first collected and in every subsequent message.

The right to object to direct marketing must be clearly, intelligibly and explicitly offered to the data subject in such a manner that it is clearly distinguishable from any other information. Where a data subject objects to direct marketing, their details should be suppressed as promptly as possible. This means that the bare minimum of their data must be retained to ensure that their direct marketing preferences are respected in the future.

Record Keeping
Under data protection law, the School is required to keep full and accurate records of all of its data processing activities. Employees must therefore keep and maintain accurate records reflecting the processing of personal data, including procedures for obtaining consent from data subjects, and records of these consents. At a minimum, these records must include the name and contact details of the School Data Protection Officer, descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, personal data retention periods, and the security measures that are in place.

Where there are any personal data breaches, records must be kept of these, including the facts surrounding the breach, the effects of the breach, and the remedial action taken.

Subject Access Requests

Introduction
Under Article 15 of the GDPR, individuals can exercise their right of access under a Subject Access Request (SAR), which allows them to see what personal information the School holds about them, whether on computer, electronic, or manual record systems. The purpose of this right of access is to allow individuals the opportunity to verify what information the School holds about them, and to confirm whether the processing of their personal data is correct and lawful.

Some data may be exempt from disclosure, and the School will notify an individual where any of their personal data has been withheld because it is the subject of an exemption. Exemptions are set out in the GDPR and Data Protection Act 2018; whether or not the School can cite an exemption often depends on why it is processing personal data. Exemptions will be considered on a case-by-case basis.

This procedure only covers requests for an individual's own personal data.

An individual may make a subject access request before exercising their other information rights under GDPR, although is not essential.

Subject Access Request Procedure
Any Subject Access Request (SAR) must be made by the individual in question.

Requests should be in writing wherever possible (I.e., letter or email). The School will make reasonable adjustments for disabled individuals where they have difficulty making an SAR in writing, for example by making a record of a verbal request.

Requests should be made to the Data Protection Officer (DPO), which is the School Registrar at:
Data Protection Officer
The London Interdisciplinary School
x + why
20-30 Whitechapel Road
London
E1 1EW
United Kingdom

dataprotection@t-lis.org

The written request should contain the following details:

- Full name;
- Date of birth;
- School department;
- Student number or School employee number, if known;
- Information you would like to access, such as
    - Student (student record, marks, counselling records, disability records, etc.)
    - Staff (HR records such as employment file, personal development discussions, safety records, etc.)
- Location where the data is likely to be held, if known
- Contact details.

It may be necessary for the School to confirm the identity of the requester, in which case the requester may be asked to provide proof of identity.

If the request is made in person or by phone to any School department, the individual will still be required to provide the above information, and the School will request that where possible the information is put in writing; again the School may require confirmation of identity.

The School will acknowledge the receipt of a subject access request in writing within 10 working days, and will provide a response within one calendar month of the receipt of the written request (provided sufficient information has been given to the School enable the School to process the request.

The response will be in writing and the information will be provided either in hard copy or electronically, depending on the preference of the requester.

A subject access right is free of charge. However, if the request to access personal data is unfounded or excessive, the School is able to charge a reasonable fee for the administrative

cost the School must incur to comply with the request, especially in cases where the request is repetitive and without reasonable justification.

Some information may contain personal data relating to third parties. The request may therefore lead to a conflict between the data subject's rights of access and the third party's rights over their own personal information. In responding to subject access requests the School will need to ensure that the rights of those third parties are not compromised by releasing the information. As the obligation on the School is to provide information rather than documents, redaction or editing may be used so that the third party information does not form part of the requested information. The School may also ask for consent from the third party. Where consent is not given, in line guidance from the Information Commissioner's Office (ICO), the School will consider whether it is reasonable in all the circumstances to disclose the email without the third party's consent.

In rare cases, the School might refuse to respond to request. This is rare and there will always be an explanation for the decision along with advice to contact Information Commissioner's Office (ICO) where the individual is dissatisfied with the outcome.

The School will confirm whether the individual's personal information is processed and provide the information requested.

In addition, the School will provide the following information within its response:

- The purpose for processing this information;
- Specific categories of personal data which is processed;
- Confirm whether the data has been or will be disclosed to third parties and/or other countries;
- Confirm data is stored according to the retention schedule;
- Individual rights applicable;
- Information about the individual's right to complain to the Office of the Independent Commissioner (ICO);
- Confirm the existence of automated decision making, including profiling, which involves the processing of the individual's personal data.

Further questions can be addressed to the Data Protection Officer (the School's Registrar) at the postal and email address above.

Subject access requests will normally be held by the School for three years after the final action.

Guidance for staff on receiving a Subject Access Request
Where a staff member receives a Subject Access Request, and:

- They have consulted this Policy;
- They have received the required information from the requester, in writing where possible, as set out in this Procedure;
- They have received proof of identity, where required;

- They have no reservations about giving out the information requested;
- The information does not include personal information about a third party who has not given consent for the information to be released;
- It is within their remit to release the information

then the staff member should release the required information to the requester. This must be done within one calendar month of receiving a valid Subject Access Request.

Where the requested information is held in another department at the School, the request should be forwarded to that department.

Where a staff member has any concern about giving out the information, they should contact the Data Protection Officer, who is the School's Registrar. Situation that may give rise to concerns include if the School is in dispute with the requester, or if the requested information includes personal data about a third party.

Roles and Responsibilities

The Board of Directors is responsible for approving and monitoring policies and procedures to ensure that the School complies with the data protection regulations.

The Chief Executive is responsible for ensuring that provisions are in place (in terms of delegated responsibilities, dedicated resourcing) to ensure that the data protection policies and procedures approved by the Board are properly implemented across the School.

Heads of Department are responsible for ensuring compliance with the GDPR and this Policy within their department, and to develop and encourage good information handling practices within their areas of responsibility. This includes undertaking Data Protection Impact Assessments (DPIAs) where appropriate, in line with this Policy and the DPIA checklist and template (Annexes 4 and 5 of this Policy). It also includes ensuring compliance with the Subject Access Request Procedure within their department. A Head of Department is the Designated Data Controller for her/his area.

Teaching and Learning Staff are responsible for ensuring their students are aware of data protection rules where their students are doing work which involves the processing of personal data (for example in research projects).

Staff members who process personal data about students, staff, applicants, alumni or any other individual must ensure that:

- All data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party;
- Personal data is kept in accordance with the School's Data Retention Schedule;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;
- Any data protection breaches are swiftly brought to the attention of the Data Protection Officer, and that the DPO is supporting in resolving such breaches;

- Subject Access Requests are dealt with in line with the Subject Access Request Procedure in this Policy, and where there is any uncertainty as to whether an information request relating to an individual's personal data should be granted, the Data Protection Officer is consulted.

All users of personal data within the School are responsible for ensuring that they process personal data in accordance with the six principles and other conditions set out in the legislation and in this policy.

The Data Protection Officer (DPO) is the School's Registrar. The responsibilities of the School's DPO are to:

- Advise the School and its staff on its obligations under the GDPR;
- Monitor compliance with this Regulation and other relevant data protection law, including providing training for all staff, monitoring training, overseeing periodic audits to ensure compliance, overseeing catastrophe testing, and ensuring GDPR compliance is built into the design of data systems;
- Report on GDPR compliance to the Board;
- Provide advice where requested on data protection impact assessments;
- Cooperate with, and act as the contact point for, the ICO;
- Operate as the first point of contact for data protection issues;
- Consult on any DPIA being conducted, and advise on whether a DPIA should be conducted. Monitor ongoing compliance with DPIAs.
- Receive and oversee the response to Subject Access Requests in line with the Subject Access Request Procedure above.

The DPO is contactable at dataprotection@t-lis.org, or Data Protection Officer, The London Interdisciplinary School, x + why, 20-30 Whitechapel Road, London, E1 1EW, United Kingdom.

Students are responsible for familiarising themselves with the Privacy Notice provided when they register with the School, and with ensuring that their personal data provided to the School is accurate and up to date.

Third Party Data Processors: Where external companies are used to process personal data on behalf of the School, responsibility for the security and appropriate use of that data remains with the School. Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures that will protect the processing of personal data;
- Reasonable steps must be taken by the School to check that such security measures are in place;
- A written contract must be in place, describing the personal data that will be processed, and for what purpose;
- A data processing agreement must be signed by both parties. This will be available from the School's Data Protection Officer.

Contractors: The School is responsible for any use of personal data made by any individual working on its behalf. Managers who employ contractors must ensure that they

are appropriately vetted for the data they will be processing. Managers must also take steps to ensure that:

- Any personal data that is collected or processed by the contractor in the course of the work undertaken for the School is kept securely and confidentially;
- All personal data is returned to the School on completion of the working, including any copies; *or* the data is securely destroyed, and the School is notified of this by the contractor;
- The School receives prior notification of any disclosure of personal data to any other third party who is not a direct employee of the contractor;
- Any personal data made available by the School, or collected in the course of the work undertaken for the School, is neither stored nor processed outside the UK, unless the School gives written consent for this to take place;
- All practical and reasonable steps are taken to ensure that contractors do not have access to personal data beyond that which is essential for the work to be carried out.

Training, Awareness and Audit

The School is committed to ensuring that all of its employees have the required training and awareness in relation to responsibilities around data protection. All employees must undergo data protection training at induction, and are required to undergo refresher training annually. The DPO has responsibility for providing training on Data Protection and ensuring that all induction members of staff undergo the training, keeping a log of training completed. Employees must regularly review all of the systems and processes under their control to ensure that they comply with this Policy.

Review and Monitoring

The Data Protection Officer (Registrar) shall review this Policy and compliance with this Policy, as well as with the associated Privacy Notices, on an annual basis (or on a more regular basis as required), and shall make a report of findings to the Board of Directors. The Board of Directors shall authorise any changes.

Annex 1: Privacy notice for students

Introduction
This privacy notice applies to applicants, current students, former students, and alumni. This notice explains how the School will process your personal data.

How do we collect your information?
The School may collect your personal data in a number of ways. These include:

- Information that you provide when engaging with us before joining, for example, when you express an interest in studying at LIS;
- When you make an application to study at LIS and complete application forms and other admissions processes and procedures, and when you interact with LIS staff. This applies whether you have applied directly to LIS, or through the Universities and Colleges Admissions Service or any other third party admissions service;
- When you communicate with LIS, for example by telephone, email or via our website;
- In a range of other ways when you interact with LIS staff as a student of LIS and in line with the purposes of data collection outlined below;
- From third parties, for example from your previous or current school, college, higher education provider or employers (such as when they are providing a reference about you or are sponsoring your studies).

What types of information do we collect?
The School may collect a range of different information, including:

- Personal details such as your name, title, date of birth, national insurance number (or other tax identification number), passport number, country of domicile, nationality, and, by consent, parental information (occupation and participation in higher education), and your eligibility for Free School Meals or Education Maintenance Allowance;
- Contact details such as home address, contact address (if different), email address and telephone number;
- Information relating to your education and employment history including the schools, colleges, higher education institutions you have attended and where you have worked, the courses you have completed, dates of study and examination results. We will also keep records relating to assessments of your work, details of examinations taken, your predicted and actual examination grades and other information in your student record;
- Special category data, as defined in the GDPR, and information about criminal convictions and offences, including:
    - Information concerning your health and medical conditions (e.g. disability and dietary needs);
    - Certain criminal convictions;
    - Information about your racial or ethnic origin; religion or similar beliefs and sexual orientation.

In addition, if you study at LIS, the data stored and processed by the College will include:

- Academic performance;
- Attendance and progression;
- Breaches of School policies such as academic or other misconduct;
- Banking and payment information.

How do we use this information?

We will only process data for specified purposes and when this is justified in accordance with our Data Protection Policy.

The table below shows examples of core purposes for the collection and processing of personal data, and the legal basis/justification for these purposes. This details that we may process your personal data primarily because it is necessary for the performance of our contract with you, or in order to take necessary pre-contractual steps.

Purpose	**Legal basis / justification**
Recruitment and promoting LIS services, e.g. providing information about programmes, Discovery Days, or other events happening on or off campus	Necessary for the School's legitimate interests and by consent for marketing.
Assessing eligibility to undertake an LIS academic programme	Necessary for the purposes of preparing to enter into a contract.
Communicating with applicants and students	Necessary for the purposes of preparing to enter into a contract and thereafter as a contractual necessity.
Assisting applicants and students to obtain residential accommodation / housing	By consent
Provision of academic programmes and related services including: • Provision of core teaching, learning and research • Assessment of academic progress and performance (including attendance) • Maintaining student records • IT • Library	Necessary to deliver on the contract to provide your chosen academic programme.
Provision of non-academic services including: • Student support • Monitoring equal opportunities • Safeguarding and promoting the welfare of students • Ensuring students' safety and security • Managing the use of social media	Necessary to deliver on the contract to provide the student experience associated with your academic programme, as well as in specific cases to protect a student's vital interests (e.g., in relation to safeguarding)
Providing appropriate IT and other infrastructure facilities, for example a virtual learning environment, as well as the development of new IT systems	Contractual necessity and the School's legitimate interest in providing a proper infrastructure to support the provision of academic programmes and related student services
Administration of complaints, grievances and appeal or to deal with any other feedback	Contractual necessity

Immigration matters	Necessary for the School to comply with its legal obligation in relation to students or applicants who hold a Tier 4 Visa. Such processing may also be in the public interest and your consent may be required in some cases.
Making reasonable adjustments for disabilities and providing relevant support to students or applicants with ill health	By consent
Regulating the School's community (including dealing with misconduct under the School's procedures for academic and other misconduct)	Contractual necessity
Obtaining payment of fees, administering finance and assessing eligibility for bursaries	Contractual necessity and the School's legitimate interest in obtaining payment for the services it provides
Protecting the School's property and assets (for example by dealing with misconduct)	Necessary for LIS's legitimate interest in safeguarding its property and assets.
Alumni relations (including fundraising)	Necessary for the School's legitimate interests and by consent for marketing, fundraising and maintaining an alumni network.
Internal audit	Necessary for the School's legitimate interests in maintaining internal control, and/or prevention, detection and investigation of fraud

We may also process your personal data because it is necessary for our or a third party's legitimate interests. For example, we may use your personal data to:

- monitor and evaluate the performance and effectiveness of the School, including by training our staff or monitoring their performance;
- maintain and improve the academic, corporate, financial, estate and human resource management of LIS;
- promote equality and diversity throughout the School;
- to seek advice on our rights and obligations, such as when we require our own legal advice.

In addition, we may also process your personal data for our compliance with our legal obligations. In this respect, we may use your personal data for the following:

- To meet our compliance and regulatory obligations, such as compliance with anti-money laundering laws and safeguarding requirements;
- For the prevention and detection of crime;
- In order to assist with investigations (including criminal investigations) carried out by the police and other authorities

There may be other processing in addition to the above, for example, when you access the LIS website which uses cookies, or when LIS takes photos or videos of you and publishes them. This is

done on the basis of our other policies and we will inform you about such processing at the time when the data is obtained or as soon as possible afterwards.

What information do we get from third parties?
In some cases, LIS will receive your information from third parties. The table below outlines core examples of the information that LIS might receive about you and where this might come from

Data LIS may receive	**Source**
Application data, which includes contact details and attainment, work experience, previous institution, contextual data and disability information	UCAS or any other third party admissions service
Your immigration status	Home Office (UKVI), Foreign & Commonwealth Office
Transcripts (details of programmes undertaken or being undertaken at another institution, and your attainment)	Another institution and/or secondary schools
Medical, accessibility related and similar information, occupational health medical clearing (we only obtain this information from third parties if you give us consent to do so)	Another institution, medical practitioners and/or family members
Your financial status	Student Loans Company or equivalent
Details of any LIS associated complaint	Office of the Independent Adjudicator
Details of performance in other educational institutions or in relevant jobs	Referees (identified by you)
Information relating to criminal convictions	Disclosure and Barring Service
Accreditation information	Relevant professional accrediting bodies

What information do we share, with whom and how?
Sometimes we may need to share your personal data. The table below gives examples of this kind of data sharing.

Recipients	**Data which we may wish to share with them**
LIS academic staff	Contact details, attendance and progression information, education and attainment data, and where necessary and subject to your consent, for the implementation of reasonable adjustments and/or the provision of other support. Your contact details may also be used by these staff when recruiting to related activities including internships .
LIS professional staff	Contact details, immigration details, attendance and progression information, education and attainment data, and where necessary and subject to your consent, for the implementation of reasonable adjustments and/or the provision of other support. Your contact details may also be

	used by these staff when recruiting to related activities including internships.
Alumni team	Contact details, attendance and progression information.
LIS Student Association	Contact details
Employers offering internships through the School	Your CV as well as any accessibility and assistance requirements (by consent, and where there is a legal basis to do so) and related information
Future employers	Personal information relating to conduct, performance and academic achievement, when asked for a reference. This will be provided by your consent.
Official bodies to which the LIS is obliged to report, for example HES, the OFS and their agents	Information supplied as necessary to fulfil School's reporting obligations to these bodies. This may include relevant special category data, and will be anonymised (and in cases where small amounts of data makes a student identifiable, the data will be suppressed).
External examiners	Exam papers
UK Home Office	Passport details, programme details and fees, and housing details
Housing providers	Student details
Data processors (e.g. third parties who process personal data on our behalf such as software providers)	Application details, attendance records
Local Authority	Contact details
Student loans company	Contact details
Research partners	Contact details, attendance
Regulatory and accrediting bodies	Contact details, attendance and progression information
Funding bodies, scholarship and bursary providers	Contact details, attendance and progression information
Government agencies, for example HMRC (only upon request and where there is a legal basis for doing so)	Contact details, attendance and progression information
Police and other crime prevention and detection agencies (only upon request and where there is a legal basis for doing so)	Contact details

How long do we keep information?

We must retain some student personal data after they leave LIS either because the law requires it or, for other reasons, e.g. to provide transcripts and references. Each type of data will be kept for a set period, which is defined in the School's Data Retention Policy and Detailed Data Retention Schedule.

Data Protection Officer

The Data Protection Officer (DPO) is the School's Registrar. The responsibilities of the School's DPO are to:

- Advise the School and its staff on its obligations under the GDPR;
- Monitor compliance with this Regulation and other relevant data protection law, including providing training for all staff, monitoring training, overseeing periodic audits to ensure compliance, overseeing catastrophe testing, and ensuring GDPR compliance is built into the design of data systems;
- Report on GDPR compliance to the Board;
- Provide advice where requested on data protection impact assessments;
- Cooperate with, and act as the contact point for, the ICO;
- Operate as the first point of contact for data protection issues.

The Data Protection Officer is contactable at dataprotection@t-lis.org.

Queries and complaints

For more information on your rights, if you wish to exercise any right, for any queries you may have, or if you wish to make a complaint, please contact the Data Protection Officer at dataprotection@t-lis.org.

Complaint to the Information Commissioner

You have the right to complain to the Information Commissioner's Office (ICO) about the way in which the School processes your personal data.

Annex 2: Privacy notice for employees

Introduction
This privacy notice applies to employees (past and present), job applicants, contractors, board members, volunteers, consultants, independent examiners and invigilators who have personal data processed by LIS.

The personal data that is processed includes personal special categories of data such as ethnicity, disability or medical data collected and data relating to criminal conviction and offences.

The notice explains how LIS will process your personal data.

LIS may update its privacy notices at any time, please check back here regularly to review changes.

What types of information do we hold?
The School holds a range of personal data about you, some of which you provide to us directly and some of which is received from third parties.

Below are some of the types of data that the School holds:

- Personal data including name, title, date of birth, gender, marital status and dependents
- Contact details including address, telephone number and personal email address
- Next of kin and emergency contact information
- National Insurance Number
- Bank account details, payroll details and tax status information
- Salary, annual leave, pension and benefits information
- Location of employment or workplace
- Recruitment information (including copies of qualifications, right to work documentation, driving license, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Immigration information (including passport details and language proficiency)
- Performance information
- Disciplinary and grievance information
- Information obtained through electronic means such as swipe card records
- Information about your use of IT systems
- ID card image, photographs, videography

The School may also collect, store and use the following special categories of more sensitive personal information:

- Information about your age, race or ethnicity, disability, religious beliefs, sexual orientation, gender, political opinions, marriage and civil partnership and pregnancy and maternity
- Information about your and your family's members' and dependents' health, including any medical conditions, general health and sickness record
- Information about criminal convictions, offences and barred list status.

How do we use this information and why?
LIS processes your personal data to help effectively administer the employment contract between you and the School. LIS only processes data for specified purposes and in accordance with Data

Protection Law and its Data Protection Policy. Some processing of personal information is justified on the basis of contractual necessity. In general, this applies to personal data you provide at the start of, and during, your employment. This information helps us to manage the employment relationship and employee performance. Without this information, LIS would be unable to follow legal requirements relating to your employment, assess your application, offer you work implement reasonable adjustments when required.

The table below outlines the legal basis/justification for key areas in which your personal data is processed. There may be other processing in addition to the below but this will always be conducted in accordance with School policies.

Purpose	**Legal basis/justification**
To decide on your recruitment or appointment	Necessary before entering into an employment contract and to comply with employment law
To determine the terms on which you work for the School	Necessary for the performance of employment contract and to comply with employment law
To allocate and manage work responsibilities (in line with the role in question)	Necessary before entering into an employment contract and to comply with employment law
To pay your salary, tax, pension contributions, and to process any relevant benefits	Necessary for the performance of employment contract and to comply with employment law
To manage training and development needs or opportunities	Necessary for the performance of employment contract
To monitor equality, diversity and inclusion	Necessary for the School's legal obligation to promote an inclusive work environment, to comply with the Equality Act 2010 and other legal obligations
To implement and ensure compliance with other School policies	Necessary for the performance of employment contracts, and to comply with LIS policy, employment law, and ICO code of practice
To assess and manage fitness and capability to work and manage sickness absence	Necessary for the performance of employment contract and to comply with employment law
To manage reviews and the promotions process	Necessary for the performance of employment contract and to comply with employment law
To provide management information and inform HR processes	Necessary for the performance of employment contract and to comply with employment law and other legal obligations and legitimate interest to ensure systems operate securely and efficiently and to inform management decisions

To communicate with you and evaluate your application as an applicant or employee	Necessary for the performance of employment contract and to comply with employment law and other legal obligations and legitimate interest in consulting with staff and raising awareness of initiatives and opportunities
To provide you with employment related benefits	Necessary for the performance of the employment contract
To liaise with your pension provider	Necessary for the performance of the employment contract and to comply with Employment Law
To sponsor international staff to work in the UK	Necessary for the performance of the employment contract and to comply with Employment Law, Immigration Law and other legal obligations
To check right-to-work status and support visa applications	Necessary for the performance of the employment contract, and to comply with employment law, immigration law and other legal obligations
To gather evidence for any potential grievance or disciplinary hearings	Necessary for the performance of employment contract, to comply with employment law
To make decisions about your employment or arrangements for the termination of the working relationship	Necessary for the performance of employment contract, to comply with employment law
To provide references on request	Necessary for the performance of employment contract or where consent has been given
To assess suitability and eligibility to undertake work	Necessary for the process of establishing a contract (contractual necessity) and in the School's legitimate interest

In cases where processing your personal data is a contractual necessity, and you don't provide LIS with the personal data needed, we may not be able to process your application or provide you with the employment for which you have been appointed.

When it comes to use of sensitive information, LIS will process this data for specified purposes and where this is justified by data protection law. The table below provides key examples.

Purpose	**Legal basis/justification**
LIS uses information about any criminal convictions, reprimands and cautions where the law allows it to do so. Where appropriate, this information will also be used to assess your suitability to carry out the work for which you are/would be engaged	Processing is necessary for the public interest and to enable LIS to meet its obligations with respect to employment law.

LIS uses information about your race, ethnicity, religious beliefs, sexual orientation and political opinions to conduct equal opportunities monitoring	Necessary for LIS's legal obligation to deliver a work environment that is inclusive and to comply with the Equality Act 2010 and other legal obligations
LIS uses information relating to your health (for example, any disability), by consent to make decisions regarding reasonable adjustment	Processing of health related data is necessary so that LIS can meet its obligations in relation to the Equality Act 2010

What information do we get from third parties?
LIS may receive your data from third parties. The table below lists the information that LIS may receive from them.

Source	**Data LIS may receive from them**
Recruiters or other employment agencies	Personal contact details, your application and CV
Former employers	Your record of previous employment
DBS provider	Your criminal record and barred list status
Relevant professional body (e.g. HEA)	Your professional registration status
Occupational health service, GPs/medical practitioners	Medical, accessibility related and similar information (by consent)
Home Office (UKVI)	Immigration status
External training providers	Training and development information
External assessment providers	Psychometric testing and assessment outcomes

What information do we share, with whom and how?
There are occasions when LIS will need to share your data. It is not possible to list all of the bodies with whom we might share your personal data. The table below outlines key examples of data sharing.

Recipient	**Data we may share**
Line managers	Contact details, employment details, attendance, performance, conduct, training, development, salary, and, by consent, health information required to ensure the School is able to fulfil its duty of care and implement reasonable adjustments when appropriate
Professional staff	Contact details, employment details, attendance, performance, conduct, training, development, salary, by consent, and health information required to ensure the School is able to fulfil its duty of care and implement reasonable adjustments when appropriate
Investigation officers, hearing panel chairs and members, external solicitors, employment tribunals	Personal information relating to conduct, performance and employment

Third party organisations which process personal data on LIS's behalf, including training providers, assessment providers and employment surveyors	Name, contact and employment details
Third parties to whom a potential TUPE transfer is being made	Employment contract terms and conditions and associated benefits (full employee liability information)
Official bodies to which LIS is obliged to report, for example, HESA, OfS, ONS or their agents	Information supplied as necessary to fulfil LIS's reporting obligations to these bodies. This may include relevant special category data
Future employers	Personal information relating to conduct, performance and employment, when asked for a reference
Professional development course tutors	Course attendance lists and contact details
Government agencies such as UK Visas and Immigration and the Home Office	Contact details, passport details, salary and other employment basis details including fixed term or permanent contract status
DBS providers	Name and contact details
Pension schemes	Personal information including contact details and salary and pension contribution details
HMRC	Contact, pay and benefit details
Professional regulatory bodies with which you have registered	Contact details, attendance and performance and conduct information.
Internal audit	Any personal data necessary for continued operation of internal controls and/or for preventing, detecting and investigating suspected fraud or irregularities
Police or other crime prevention and detection agencies	Information will be supplied as necessary to fulfil legal obligations with respect to the prevention and detection of crime

How long do we keep information?
We must retain some staff personal data after they leave LIS either because the law requires it or, for other reasons, e.g. tax reasons. Each type of data will be kept for a set period, which is defined in the School's Data Retention Policy and Detailed Data Retention Schedule.

Data Protection Officer
The Data Protection Officer (DPO) is the School's Registrar. The responsibilities of the School's DPO are to:

- Advise the School and its staff on its obligations under the GDPR;
- Monitor compliance with this Regulation and other relevant data protection law, including providing training for all staff, monitoring training, overseeing periodic audits to ensure compliance, overseeing catastrophe testing, and ensuring GDPR compliance is built into the design of data systems;
- Report on GDPR compliance to the Board;
- Provide advice where requested on data protection impact assessments;
- Cooperate with, and act as the contact point for, the ICO;
- Operate as the first point of contact for data protection issues.

The Data Protection Officer is contactable at dataprotection@t-lis.org.

Queries and complaints
For more information on your rights, if you wish to exercise any right, for any queries you may have, or if you wish to make a complaint, please contact us the Data Protection Officer at dataprotection@t-lis.org.

Complaint to the Information Commissioner
You have the right to complain to the Information Commissioner's Office (ICO) about the way in which the School processes your personal data.

Annex 3: Privacy notice for visitors

Introduction
This Privacy Notice applies to visitors to LIS and people with whom the School communicates who are neither staff, nor current students, nor applicants, nor alumni, nor board members. It does apply to prospective applicants (e.g. enquirers), prospectus requesters, event registrants and attendees, external speakers, and all other individuals who have expressed an interest in: studying at LIS; participating in its activities in another way, such as one of LIS' outreach programmes; and one off events, e.g. Discovery Days. This notice also applies to agents, third parties and partners, as well as employers. This notice explains how LIS will process your personal data.

This notice explains how the School will process your personal data. LIS may update its Privacy Notice at any time; please check back here regularly to review any changes.

What types of information do we hold?
LIS holds a range of personal data about you. Some of this is provided to you directly and some of this is received from third parties such as agents or third-party companies. Sometimes this means LIS may process information related to children in your care.

Examples of the categories of personal data which the School holds, include:

- Personal details including name and title
- Contact details including address, telephone number and email address
- Country of nationality and domicile
- Company details
- Study interests
- Qualifications
- Academic institutions attended

LIS may also, by consent, collect, store and use information about your health or religion should you require it to make reasonable adjustments for you during your visit to LIS or to make resources accessible.

How do we use this information and why?
LIS processes your data to help support your current and future relationship with the School. We only process your data for specified purposes and if it is justified in accordance with data protection law and the School's Data Protection Policy. The table below lists various purposes for which LIS processes personal data and the corresponding justification for this.

It is not possible to capture all purposes for which LIS processes your data and there may be other processing in addition to the below. This is undertaken in accordance with LIS's policies, of which LIS will inform you when the data is obtained or as soon as possible thereafter.

Data Subject	Data processed and purpose of this	Legal basis and justification
Visitors to LIS for commercial, community or similar purposes	Name and contact details	Processing is necessary for LIS's legitimate interest in regulating access to the site and managing safety within it

Members of the general public who visit LIS for a specific event	Name, contact details, and any other information required for your attendance at the event, such as dietary requirements	Contractual necessity - without this personal data, LIS may not be able to deliver the event for you
Contractors providing services to LIS	Name and contact details	Contractual necessity – without the personal data, LIS may be unable to comply with its legal obligations to ensure the health and safety of visitors to its site and so will be unable to allow you onto its premises to perform the contract
Individuals with whom LIS corresponds, including schools, businesses or recruitment agents	Name and contact details. LIS uses your data to keep you up to date with events and initiatives which may be of interest and/or benefit to you	Processing is necessary for LIS's legitimate interest in providing you information on items which may be of interest or benefit
Members of research communities and collaborators	Contact details to maintain research communities and sharing research-related news and best practice	Public task
Members of the public using LIS facilities	Name, contact details, area of interest, country of nationality and domicile. The LIS uses your data to respond to your enquiry and/or to provide a prospectus	Contractual necessity
Prospective applicants who enquire to LIS, request information at an event or request a prospectus	Name, contact details, enquiry/area of interest, country of nationality and domicile. LIS uses your data to respond to your enquiry and/or to provide a prospectus	For answering your question, the legal basis for processing is contractual necessity. You may also be sent information regarding LIS' events, educational programmes or resources if this would relevant to potential future study
Individuals applying for/booking on a LIS Discovery Day, or equivalent open day style event	Name, contact details, date of Birth, address, gender, nationality, school/college/educational background, and, by consent: eligibility for Free School Meals, Eligibility for Education Maintenance Allowance, parental HE attendance, disability information, dietary requirements, whether you have been or are in care	For processing your application/reservation, making reasonable adjustments in delivery, and for better understanding the reach and potential impact of our efforts to broaden higher access and participation, as required by the Office for Students as a condition of registration.

		You may also be sent information regarding LIS's events, educational programmes or resources if this would be relevant to potential future study, and by consent.
Enquiry data collected via third party platforms, such as UCAS, What Uni?, the The Student Room, etc.	Name, contact details, area of interest, school/college/educational background and further information supplied by the third party, which may vary. LIS uses this data to send relevant marketing materials of interest.	The legal basis for processing is consent. You may also be sent information regarding LIS events, educational programmes or resources if this would be relevant to potential future study. Some of this information may also be used as a contractual necessity in its relationship with you.

There may be other processing in addition to the above, for example, when you access the LIS website which uses Cookies, or when LIS takes photos or videos at events and then publishes them. This is done on the basis of our other policies, and LIS will inform you about such processing at the time when the information is obtained or as soon as possible thereafter. For example, we will request consent before publishing photos or videos of you.

What information do we get from third parties?
There are occasions when LIS receives your data from third parties. The following table lists key examples of information the School may receive from them.

Source	**Data we may receive from them**
Schools arranging a visit or engaging in another programme, or providing references for those participating	Personal and contact details and information relating to your background and living situation when this is necessary for eligibility purposes
Other institutions arranging a visit	Personal and contact details
Your employer	Personal and contact details and employment role
Third party marketing companies and recruitment agents	Personal and contact details
UCAS media	Personal and contact details

What information do we share, with whom and how?

Recipients	**Data that we may share with them**
LIS' administrative and support staff	Personal and contact details and, if necessary, for the implementation of reasonable adjustments and/or the provision of other support and, subject to your consent, health information

Data processors (third parties who process personal data on LIS' behalf)	Personal and contact details
Local Authorities	Relevant safeguarding information
Scheme funders or research partners	Contact details, attendance and progression information, and information relating to your background and living situation where necessary for eligibility purposes

How long do we keep information?
We must retain some student personal data after they leave LIS either because the law requires it or, for other reasons, e.g. to provide transcripts and references. Each type of data will be kept for a set period, which is defined in the School's Data Retention Policy and Detailed Data Retention Schedule.

Data Protection Officer
The Data Protection Officer (DPO) is the School's Registrar. The responsibilities of the School's DPO are to:

- Advise the School and its staff on its obligations under the GDPR;
- Monitor compliance with this Regulation and other relevant data protection law, including providing training for all staff, monitoring training, overseeing periodic audits to ensure compliance, overseeing catastrophe testing, and ensuring GDPR compliance is built into the design of data systems;
- Report on GDPR compliance to the Board;
- Provide advice where requested on data protection impact assessments;
- Cooperate with, and act as the contact point for, the ICO;
- Operate as the first point of contact for data protection issues.

The Data Protection Officer is contactable at dataprotection@t-lis.org.

Queries and complaints
For more information on your rights, if you wish to exercise any right, for any queries you may have, or if you wish to make a complaint, please contact us the Data Protection Officer at dataprotection@t-lis.org.

Complaint to the Information Commissioner
You have the right to complain to the Information Commissioner's Office (ICO) about the way in which the School processes your personal data.

Annex 4: Checklist to determine whether or not a Department should conduct a Data Protection Impact Assessment

Based on guidance from the Information Commissioner's Office (ICO)

This checklist is intended to support staff in determining whether a Data Protection Impact Assessment (DPIA) should be conducted for a new process, activity or project or major change to an existing process, activity or project involving the processing of personal data.

Staff should consider carrying out a Data Protection Impact Assessment where any of the following apply:

- The activity is a major project involving the use of personal data
- The activity involves evaluation or scoring
- The activity involves automated decision-making with significant effects
- The activity involves systematic monitoring
- The activity entails processing of sensitive data or data of a highly personal nature
- The activity entails large scale data processing
- The activity entails processing of data concerning vulnerable data subjects
- The activity comprises innovative technological or organisational solutions
- The activity comprises processing that involves preventing data subjects from exercising a right or using a service or contract

Where a Department determines not to undertake a DPIA in relation to a new project, activity or process that involves the processing of personal data, they must document their reasons for not doing so.

Staff must conduct a Data Protection Impact Assessment where any of the following apply:

- The activity involves using systematic and extensive profiling, or automated decision-making about individuals
- The activity involves processing special-category data or criminal-offence data on a large scale
- The activity involves the systematic monitoring of a publicly accessible place on a large scale
- The activity comprises the use of innovative technology in combination with any of the criteria in the European guidelines
- The activity uses profiling, automated decision-making or special category data to help make decisions on an individual's access to a service, opportunity or benefit
- The activity carries out profiling on a large scale
- The activity processes biometric or genetic data in combination with any of the criteria in the European guidelines
- The activity combines, compares or matches data from multiple sources

- The activity processes personal data without providing a privacy notice directly to the individual, in combination with any of the criteria in the European guidelines
- The activity processes personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines
- The activity processes children's personal data for profiling or automated decision-making or marketing purposes, or offer online services directly to them
- The activity processes personal data that could result in a risk of physical harm in the event of a security breach
- There is a change to the nature, scope, context or purposes of the School's processing

Annex 5: Data Protection Impact Assessment Template
From the Information Commissioner's Office (ICO)

Where a Department or member of staff determines that a Data Protection Impact Assessment (DPIA) should be undertaken for a new project, activity or process involving the processing of personal data, or a significant change to an existing activity or process that involves the processing of personal data. Staff should us the School's DPIA Checklist in making this determination.

This template enables staff to record the process and outcome of a DPIA. Once completed, the outcomes of the DPIA should be incorporated into the project plan.

1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
2. Describe the processing
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current

state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

3. Describe consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

4. Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights?
What measures do you take to ensure processors comply? How do you safeguard any international transfers?

5. Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include	**Likelihood of harm**	**Severity of harm**	**Overall risk**

associated compliance and corporate risks as necessary			
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

6. Identify measures to reduce risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, medium or high	Yes/no

7. Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments		

Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Name of policy/procedure:	**Data Protection Policy and Privacy Notices**
Document owner:	**Hannah Kohler, Director of Admissions and Student Support**
Date Originally Created:	**01/2019**
Last reviewed:	**06/2019**
Reviewed by:	**Plum Turner (Director of Marketing and Recruitment)** **Jasper Joyce (Director of Finance and Operations)**
Audited by:	**Board of Directors**
Date of Audit:	**11/2019**
Date of next review: (annually unless otherwise agreed)	**11/2020**
Related documents: (e.g. associated forms, underpinning processes, related policies or overarching policies)	**Data Retention Policy** **Detailed Data Retention Schedule** **Staff Training Programmes and Logs**

Version Control			
Version	**Author**	**Date**	**Brief summary of changes**
1	**Hannah Kohler (Director of Admissions and Student Support)**	**13/01/2019**	**Original draft**
2	**Jasper Joyce (Director of Finance and Operations) & Plum Turner (Director of Marketing and Recruitment)**	**29/01/2019**	**Clarification of accountabilities of Board; contact info of DPO; clarification on student consent**
3	**Jasper Joyce (Director of Finance and Operations)**	**12/03/2019**	**Small changes to wording**
4	**Jasper Joyce (Director of Finance and Operations)**	**07/05/2019**	**Small changes to wording**

5	**Hannah Kohler (Director of Admissions and Student Support)**	**21/06/2019**	**Identification of Data Protection Officer and inclusion of dedicated email address. DPO responsible for delivering and monitoring training. Added Privacy Notices (also included on website); included Subject Access Request procedure. Included DPIA checklist and template and expanded on procedure for DPIA in main policy document**
6	**Board of Directors**	**18/11/2019**	**Approved.**