The London Interdisciplinary School

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.

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.

This policy is not part of the formal contract between the School and its staff or students. However, compliance with this policy is a condition of employment and of the Student Contract; any breach of the policy may therefore lead to disciplinary proceedings under the Student or Staff Disciplinary Procedures.

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 will be registered with the ICO.

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.

<u>GDPR Principle 2: Purpose Limitation</u>

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 pseudonumisation.

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.

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.

<u>Privacy By Design and Default</u>

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.

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.

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. The School's IT Security Policy and Programme supports 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 Regulation).

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 Information Commissioner's Office 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 Schedule that has been developed in line with legal and business requirements.

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 placements partner to support the School's placements programme, the student will be asked to sign another consent form.

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 research must give proper consideration to this policy. These 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.

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, the DPA and this policy within their department, and to develop and encourage good information handling practices within their areas of responsibility. 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.

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.

Data Protection Officer: At the point of registration as a higher education provider with the Office for Students, the School will have in place a Data Protection Officer. Their responsibilities will be 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 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 Information Commissioner's Office;
- Operate as the first point of contact for data protection issues.
- The School's Data Protection Officer will be contactable at a dedicated email address, once appointed

In the interim, an appropriate internal member of staff will adopt the responsibilities of the DPO as outlined above. This member of staff will be contactable at hello@t-lis.org and the email subject should be marked "Data Protection".

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. Employees must regularly review all of the systems and processes under their control to ensure that they comply with this data protection policy.

Policy Changes

The Board of Directors shall review this policy annually or on a more regular basis as required and shall authorise any appropriate changes.

Name of policy/procedure:	**Data Protection Policy**
Document owner:	**Hannah Kohler, Head of Student Experience**
Date Originally Created:	**01/2019**
Last reviewed:	**03/2019**
Reviewed by:	**Plum Turner (Head of Marketing)** **Jasper Joyce (Head of Strategy and Finance)**
Audited by:	**[name and job title]**
Date of Audit:	**MM/YYYY**
Date of next review: (annually unless otherwise agreed)	**MM/YYYY**
Related documents: (eg associated forms, underpinning processes, related policies or overarching policies)	**Data Retention Schedule**

Version Control			
Version	**Author [name]**	**Date**	**Brief summary of changes**
1	**Hannah Kohler (Head of Student Experience)**	**13/01/2019**	**Original draft**
2	**Jasper Joyce (Head of Strategy and Operations) & Plum Turner (Head of Marketing)**	**29/01/2019**	**Clarification of accountabilities of Board; contact info of DPO; clarification on student consent**
3	**Jasper Joyce**	**12/03/2019**	**Small changes to wording**

4	**Jasper Joyce**	**07/05/2019**	**Small changes to wording**