TEDI-LONDON

PRIVACY AND DATA PROTECTION POLICY

Summary	The aims of this policy are to: 1. Set out the expectations and procedures in relation to how personal data is processed at TEDI-London. 2. Ensure TEDI-London complies with data protection legislation and best practice 3. Minimise the risk to TEDI-London of personal data breaches and other breaches of data protection legislation		
Policy Owner	Director of Resources		
Policy Sponsor	CEO		
Policy applies to	All staff at TEDI-London		
Equality impact assessment completed	This policy, and the privacy and data protection legislative framework acknowledge that personal data relating to individuals with protected characteristics under the Equality Act 2010 needs to be carefully managed and controlled. Such data is deemed Special Category Personal Data as it is likely to be more sensitive, or private, and therefore likely to cause more damage or distress if compromised. It is therefore given additional protection in data protection legislation and this policy.		
Relevant Legislation and Policies	General Data Protection Regulation (GDPR) Data Protection Act 2018 TEDI-London Privacy Notice Equality Act 2010		
Version	1		
Approved by	Executive	**Approval date**	February 2021
Date of implementation	February 2021	**Date of next formal review**	February 2024

DOCUMENT CONTROL

Date	Version	Action	Amendments
17/02/21	1	Approved	
23/08/21	2	Updated	Specific reference at 5.6 to students allowing TEDI-London to share their data with third parties.

Contents

1. INTRODUCTION

1.1. TEDI-London is committed to protecting the privacy and security of personal data belonging our staff, students, and other stakeholders in accordance with our obligations under the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any UK legislation relating to the protection of personal data and the privacy of individuals.

1.2. This policy sets out the roles and responsibilities of TEDI-London and its officers regarding the collection, processing, security of and access to personal data, detailing governance and due diligence arrangements and the framework for investigating and preventing data breaches.

2. POLICY STATEMENT

2.1. The aims of this policy are to:

1. Set out the expectations and procedures in relation to how personal data is processed at TEDI-London.
2. Ensure TEDI-London complies with data protection legislation and best practice.
3. Minimise the risk to TEDI-London of personal data breaches and other breaches of data protection legislation.

2.2. In order to achieve these aims, and in accordance with the GDPR's data protection principles (refer Appendix A) and data subject rights, TEDI-London will:

1. Embed data protection and privacy by design so that data protection and privacy issues are considered upfront in our activities.
2. Process personal data in a lawful, fair and transparent manner.
3. Ensure that personal data is collected for specific, explicit and legitimate purposes and that data is limited to that necessary for the purposes it is collected and processed.
4. Maintain personal data that is accurate and up-to-date, correcting or deleting inaccurate data.
5. Inform data subjects of the lawful basis and explain the purpose and manner of the processing in the form of privacy notices and other similar methods.

6. Only keep personal data in an identifiable format for as long as necessary (noting the exceptions for public interest, scientific, historical or statistical purposes).

7. Maintain confidentiality and keep personal data secure.

8. Ensure staff are trained appropriately in managing personal data

9. Not share personal data with third parties unless adequate standards of data protection can be guaranteed and, where appropriate, contractual arrangements are put in place

10. Implement comprehensive and proportionate governance measures to demonstrate compliance with data protection legislation principles

11. Observe the rights of individuals under data protection legislation (Refer Appendix A)

3. SCOPE OF THIS POLICY

3.1. This policy applies to all TEDI-London activities and processes in which personal data is used, regardless of whether it is in a digital or hard copy format.

3.2. This policy applies to TEDI-London staff and students and to others acting for or on behalf of TEDI-London who are granted access to our information infrastructure.

4. DEFINITIONS

4.1. Data Controller: A person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data. TEDI-London is the data controller for the purposes of this policy. A data controller remains responsible for a data processor's use of information which is passed to a data processor by the data controller and must take steps to ensure that processors are able to protect personal data before providing it.

4.2. Data Processor: A person, public authority, agency or other body that processes personal data on behalf of the data controller, for example agents and contractors (not an employee of the data controller).

4.3. Data Protection Officer: The person responsible for informing and advising TEDI-London about its data protection obligations and for monitoring TEDI-London's compliance with them. At TEDI-London the Data Protection Officer is the Director of Resources (dpo@tedi-london.ac.uk).

4.4. Data Subject: The identified or identifiable living individual to whom personal data relates.

4.5. Personal Data: Any information relating to a person (data subject) who can be identified, directly or indirectly, through an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. TEDI-London processes personal data relating to a number of categories of data subject, including employees, students, applicants, business contacts, visitors, suppliers and contractors.

4.6. Personal Data Breach: A security incident that has affected the confidentiality, integrity or availability of personal data. A personal data breach occurs whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or is made unavailable and this unavailability has a significant negative effect on individuals.

4.7. Processing: In relation to personal data, processing means almost anything TEDI-London might do with personal data or sets of personal data (whether or not by automated means) such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

4.8. Special Category Personal Data: Personal data that is likely to be more sensitive, or private, and therefore likely to cause more damage or distress if compromised. It is therefore given additional protection in data protection legislation. The categories are:

1. personal data revealing racial or ethnic origin;
2. personal data revealing political opinions;
3. personal data revealing religious or philosophical beliefs;
4. personal data revealing trade union membership;
5. genetic data;
6. biometric data (where used for identification purposes);
7. data concerning health;
8. data concerning a person's sex life and
9. data concerning a person's sexual orientation.

5. ROLES AND RESPONSIBILITIES

5.1. The Executive is responsible for ensuring Privacy and Data Protection Policies are in place and that suitable controls are in operation to monitor and comply with our legislative responsibilities in these areas.

5.2. The Data Protection Officer (The Director of Resources) is responsible for:

5.2.1 Informing and advising TEDI-London about its data protection obligations and responsibilities.

5.2.2 Ensuring TEDI-London staff are aware of and trained in data protection.

5.2.3 Monitoring compliance within TEDI-London and commissioning regular reviews and audits to monitor compliance and ensure improvement recommendations are actioned.

5.2.4 Providing advice and reviewing data protection impact assessments (refer Appendix 2)

5.2.5 Ensuring all subject access requests are processed at TEDI-London and all personal data breaches investigated in accordance with Section 8 of this policy.

5.2.5 Cooperating with the Information Commissioner's Office (ICO) as required and acting as the contact point for any issues relating to data protection.

5.3. The Leadership Team is responsible for:

5.3.1 Taking responsibility for data protection compliance within their functional areas.

5.3.2 Ensuring their staff involved in data processing have completed TEDI-London's mandatory online GDPR training within the last two years.

5.3.3 Ensuring that any contractors, short term or voluntary staff that are employed in their portfolios are appropriately vetted for the data they will be processing, are not given access to personal data other than that which is essential for the work they are undertaking and have undertaken appropriate GDPR training. Any personal data collected or processed for TEDI-London by contractors, short term or voluntary staff must be kept securely and confidentially and either returned to TEDI-London on completion of the work or securely destroyed in consultation with TEDI-London.

5.4. The Chief Information Officer is responsible for:

5.4.1 Managing information security across TEDI-London to ensure risk assessment, mitigation and review with regard to information security (refer IT Usage Policy).

5.4.2 Assist the Data Protection Officer in relation to system-related DPIAs, data breaches and data subject access requests.

5.5. TEDI-London Staff:

5.5.1 All TEDI-London staff must complete the mandatory online GDPR training course and ensure they refresh this training every two years.

5.5.2 Our staff who process personal data must ensure that:

a. all information processed is necessary for the purpose for which it is required;

b. all personal data is kept securely in line with the IT Usage Policy;

c. no personal data is disclosed (accidentally or otherwise), to any unauthorised third party;

d. personal data is kept in accordance with approved data retention schedules which, at TEDI-London, are our Staff and Student Registers of Processing Activities (ROPAs) (see Appendix D);

e. any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer (Director of Resources) (dpo@tedi-london.ac.uk);

f. any personal data protection breaches are promptly brought to the attention of the Data Protection Officer as soon as possible (dpo@tedi-london.ac.uk) (refer section 8);

g. advice is sought from the Data Protection Officer if there is uncertainty about a data protection matter (dpo@tedi-london.ac.uk);

h. they notify their line manager and the Data Protection Officer immediately if they believe this policy has been breached.

5.5.3 To assist staff in fulfil their data protection obligations, Appendix A sets out the principles for processing personal data that we will adhere to.

5.6. TEDI-London Students:

5.6.1 Students will be made aware of the Privacy Notice and Privacy and Data Protection Policy to ensure that:

- they are aware how their data will be collated and managed;
- they respect the privacy and personal data of staff, students, industry and community members working alongside them at TEDI-London;
- they know who to report or escalate a suspected personal data breach to (refer 7.2.1).

5.6.2 Students will be required to give us explicit permission to share their data with third parties such as King's College London and the Higher Education Statistics Agency (HESA). Further information about why we collect this data is available within the Privacy Notice, the Data Sharing Agreement and the Register of Processing Activities (ROPA).

5.6.3 Students should make sure that the personal data they provide to TEDI-London is up-to date and accurate.

6. PRIVACY NOTICE

6.1. In order to inform our staff, students and the wider community about our commitment to privacy and data protection; to detail the types of personal data we may collect; and to explain how we store and handle personal data, TEDI-London will publish a Privacy Notice on its website.

6.2. The Privacy Notice covers the following information:

6.2.1 Who we are, our aims and objectives;

6.2.2 Key definitions, a summary of our legal obligations and contact details;

6.2.3 Details regarding when and how we will collect data, and the lawful bases we will rely on to process it;

6.2.4 Our use of cookies;

6.2.5 Data subject rights; and

6.2.6 Additional information about how we use data including data retention and sharing of your data.

6.3. The Privacy Notice will be updated from time to time and past versions of this Privacy Notice are available by request to the Data Protection Officer (data.request@tedi-london.ac.uk).

6.4. As set out in the TEDI-London Privacy Notice, you have the right to receive copies of your personal data held by TEDI-London and can do so by request to the Data Protection Officer (data.request@tedi-london.ac.uk).

6.5. Further information about your rights is available from the Information Commissioner's Office

7. DATA PROTECTION IMPACT ASSESSMENTS

7.1. As part of our commitment to privacy and data protection by design and in order to meet individuals' privacy expectations, TEDI-London will use data protection impact assessments (DPIAs) to help identify and reduce data protection risks relating to our processes, to specific projects and to any arrangements TEDI-London has in place with data processors.

7.2. Processes for which DPIAs will be completed include the use of new technologies for data processing which may be likely to result in a high risk to the rights and freedoms of individuals. This may include (but is not limited to) systematic and extensive processing activities, large scale processing of special category personal data, third-party involvement in data processing and the use of CCTV.

7.3. As a data controller, TEDI-London remains responsible for the use of information it has passed to a data processor and must take steps to ensure that a data processor is able to protect personal data before providing it them. A DPIA will be undertaken by the relevant portfolio in TEDI-London in consultation with the Data Protection Officer.

7.4. A template for DPIAs is available at Appendix B. DPIAs will be discussed with and approved by the Dean / CEO of TEDI-London.

7.5. A register of DPIAs will be maintained by the Data Protection Officer and DPIAs will be made available to the Information Commissioner on request.

8. CONTRACTS WITH THIRD PARTIES

Data Sharing Agreements

8.1. TEDI-London is required to put in place a data sharing agreement with third party data controllers. This helps everyone to understand the purpose for sharing data, what will happen at each stage and what responsibilities the parties have.

8.2. A data sharing agreement will include details about:

8.2.1 the parties' roles;

8.2.2 the purpose of the data sharing;

8.2.3 what is going to happen to the data at each stage;

8.2.4 regular reviews to ensure information and processes remain up-to-date and appropriate.

8.3. Anyone wishing to make a data sharing agreement should first speak to the DPO to ensure that an appropriate template is used. A DPIA must also be completed (refer Section 7 and Appendix B)

8.4. A register of Data Sharing Agreements will be maintained by the Data Protection Officer and Data Sharing Agreements will be made available to the Information Commissioner on request.

Written Contracts with Data Processors

8.5. TEDI-London is required to put in place a written contract with any data processors. Anyone wishing to appoint a data processor should first speak to the DPO to ensure that an appropriate contract is used. A DPIA must also be completed (refer Section 7 and Appendix B)

8.6. Written contracts with data processors shall include the following details relating to the data processing:

8.6.1 subject matter of the processing;

8.6.2 duration of the processing;

8.6.3 nature and purpose of the processing;

8.6.4 type of personal data involved;

8.6.5 categories of data subject; and

8.6.6 controller's obligations and rights (in accordance with the list set out in Article 28(3) of the UK GDPR)

8.7. The DPO will maintain a register of all current processor contracts, which will be updated when processors change.

8.8. If a data processor uses a sub-processor to help with the processing it is doing on TEDI-London's behalf, written authorisation from TEDI-London and a written contract with that sub-processor will be put in place.

9. PERSONAL DATA BREACHES

9.1. TEDI-London will ensure that personal data is kept secure. To do this we will implement appropriate technical measures (e.g. encryption, access control) and ensure our staff are aware of and trained in data protection principles and practices so as to avoid unauthorised or unlawful processing and the accidental loss, destruction or damage of personal information.

9.2. Should a personal data breach occur, TEDI-London will manage the incident efficiently and effectively as follows:

9.2.1 All suspected and actual data breaches will be reported to the Data Protection Officer (the Director of Resources) and the Chief Information Officer (if the data breach is related to IT systems) as soon as possible. Staff can escalate an actual or suspected breach via their supervisor and students can escalate an actual or suspected breach via Student Hub in the Registry. Reports should be made as a matter of urgency. A data breach reporting form is at Appendix B together with examples of personal data breaches that need to be reported,

9.2.2 In the first instance, the DPO (and CIO if appropriate), with the assistance of relevant staff members, will control and contain any data breaches to recover data, prevent further breaches and minimise harm.

9.2.3 The DPO will then:

a. assess the risks associated with data breach to determine the next steps in terms of containing the breach;

b. notify relevant parties (taking into account legal, regulatory and contractual notification requirements as well as the need to notify data subjects who may have been affected);

c. take steps to prevent further breaches occurring by implementing specific and systemic improvements;

d. consider whether any staff disciplinary or student misconduct procedures need to be instigated where there evidence of non-compliance with this policy; and,

e. ensure records of the data breach and TEDi-London's response are maintained and that the effectiveness of TEDI-London's response is reviewed by the Executive.

10. SUBJECT ACCESS REQUESTS

10.1. Data subjects are entitled to ask TEDI-London to provide a copy of any information that TEDI-London holds about them. The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of all personal data that TEDI-London holds about them.

10.2. Subject Access Requests can be made to the DPO (data.request@tedi-london.ac.uk) but can be made via any channel (email, letter, over the phone, even via social media.

10.3. The DPO will process requests in accordance with the legislation.

10.4. Staff are required to assist the DPO in providing relevant information as a priority. This is because we must comply with a subject access request, 'without undue delay' and, at the latest, within one month of receipt of the request (unless the request is complex or there are multiple requests).

10.5. In certain circumstances, TEDI-London can charge an administrative fee which can take into account factors including who is processing the information, the costs of locating, retrieving and extracting the information, the costs of communicating and providing copies of the information etc. the DPO will determine whether a fee will be charged and what a reasonable fee will be.

10.6. If anyone (for example, the Police or the spouse or parent of a data subject) requests access to personal data relating to another person, staff must first check with their line manager or the DPO (dpo@tedi-london.ac.uk) before making a disclosure.

10.7. Further information about data subject rights is accessible via TEDI-London's Privacy Notice.

11. PROVIDING REFERENCES

11.1. TEDI-London staff who give references (which should be written in all cases) should ensure they contain only information that is factual or is an honest opinion or judgement that is capable of being demonstrated as being reasonable by reference to actions or events. It should also be clear in what capacity you are providing the reference.

11.2. In respect of references for current or past employees of TEDI-London, you should inform the People Team of the request and an agreed written reference will be provided and retained on the relevant staff member's personnel e-file.

11.3. In respect of references for TEDI-London students, you should inform the Registry of the request and an agreed written reference will be provided and retained on the relevant student's record.

11.4. Referees should be aware that confidential references are exempted from data subject access requests under data protection legislation, although this may be overridden in the unlikely event of a relevant court case or legal action (which could potentially result in you personally and/or TEDI-London being held liable for losses incurred should the reference be found to be inaccurate).

12. DATA GOVERNANCE AND TRAINING

12.1 TEDI-London will demonstrate compliance with data protection legislation principles through the following governance arrangements:

12.1.1 An annual report on data protection compliance, in additional to reports of any data breach incidents that require reporting to the ICO and the results of data compliance reviews and audits, will be made to the Audit, and Risk Committee of the Board of Trustees.

12.1.2 The appointment of the Director of Resources as Data Protection Officer to inform and advise TEDI-London about its obligations to comply with data protection legislation, to monitor compliance, and to be the first point of contact for the Information Commissioner and for individuals whose data is processed.

12.1.3 TEDI-London will maintain records of its processing activities, data breach incidents and their management and will ensure data protection impact assessments (DPIAs) are in place for any significant data processing activities, particularly those involving third-parties which will be made available to the Information Commissioner on request.

12.1.4 TEDI-London will adhere to the principles of privacy and data protection by design (designing projects, processes, products or systems with privacy in mind at the outset). Relevant actions could include: Data minimisation, data anonymisation, transparency, continuous improvement regarding data security, implementation and review of DPIAs.

12.1.5 TEDI-London will publish and keep updated a Privacy Notice on its website informing data subjects and the wider community about our commitment to privacy and data protection; the types of personal data we may collect; and information about how we store and handle personal data.

12.2 TEDI-London will ensure our staff are trained about data protection and managing personal data via our online data protection training course within one month from the date of commencing employment and then regularly every two years. Training completion rates will be monitored by the Data Protection Officer.

12.3 The Data Protection Officer will also provide or arrange tailored training and advice on request and if data protection issues are identified with regard to particular areas or processes.

12.4 The Privacy and Data Protection Policy will be disseminated to staff and students via the TEDI-London website. Staff, students and data subjects can contact the Data Protection Officer with any data protection queries (dpo@tedi-london.ac.uk).

13 MONITORING AND REVIEW

13.1 The Director of Resources, as the Data Protection Officer, will ensure that compliance with the policy is monitored.

13.2 The Policy will be reviewed every three years.

APPENDIX A: Data Protection Principles and Data Subjects Rights Explained

Data Protection Principles

Principle	Requirement and what we will do
Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. We will provide the data subject with information about his/her personal data processing in a concise, transparent and intelligible manner, which is easily accessible, distinct from other undertakings between TEDI-London and the data subject, using clear and plain language. If we need to transfer personal data outside of the EEA, we will ensure that it is adequately protected in accordance with legal requirements.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will regularly review the purposes for which we use personal data and will take steps to inform the data subject in advance of any changes to those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. We will ensure that we collect enough data to achieve our purposes but not more than needed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date. We will take reasonable steps to delete or amend inaccurate or outdated data.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. We will implement technical and organisational measures to ensure that we only retain personal data where we have a legal ground to so.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. We will assess risk, implement appropriate security for personal data and check on a regular basis that our security is up to date and working effectively. All data processors appointed by TEDI-London will be assessed against their ability to adequately protect personal data and we will have formal agreements in place with them.
Accountability	The controller shall be responsible for and be able to demonstrate compliance with the data protection legislation. We will maintain records of our compliance and undertake periodic audits to ensure we continually improve our processes and measures to protect personal data.

Data Subject Rights

Right provided by GDPR	Notes
Right to be informed **We will provide privacy notices when collecting personal data from data subjects (via websites, forms, emails)**	If data is obtained directly from the data subject, the information should be provided at the time of collection of the data. If data is not obtained directly the information should be provided: • within a reasonable period of obtaining the data (within one month); • if the data are used to communicate with the data subject, at the latest, when the first communication takes place; and • if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
Right of access **Data subjects have the right to obtain:** • **confirmation that their data is being processed;** • **access to their personal data; and** • **other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.**	Information must be provided without delay and at the latest within one month of receipt. TEDI-London will be able to extend the period of compliance by a further two months where requests are complex or numerous. If so, we must inform the individual within one month and explain why. **All requests must be passed immediately to the DPO.** This right only allows access to their personal data (with some permissible exceptions).
Right to rectification **Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.**	We must respond within one month or, if the request is complex, this can be extended by two months. If we are not taking any action, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. **All requests must be passed immediately to the DPO.**
Right to erasure **A data subject may request the erasure of personal data where:** **the personal data:** • **is no longer necessary in relation to the purpose for which it was originally collected/processed** • **was unlawfully processed** • **has to be erased in order to comply with a legal obligation** • **is processed in relation to the offer of information society services to a child**	We can refuse to comply with a request for erasure where the personal data is processed: • to exercise the right of freedom of expression and information; • to comply with a legal obligation or for the performance of a public interest task or exercise of official authority; • for public health purposes in the public interest; • for archiving purposes in the public interest, scientific research historical research or statistical purposes; or • for the exercise or defence of legal claims. **All requests must be passed immediately to the DPO.**

Right provided by GDPR	Notes
the individual: • **withdraws consent** • **objects to the processing and there is no overriding legitimate interest for continuing the processing**	
Right to restrict processing **Processing must be suppressed where:** • **the individual contests the accuracy of the personal data;** • **an individual has objected to the processing (where it was necessary for performance of a public interest task or legitimate interests);** • **processing is unlawful and the individual requests restriction instead of erasure;** • **you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.**	We can continue to store the personal data, but may only further process it: • with the data subject's consent; • to establish, exercise, or defend legal claims; • to protect the rights of another individual or legal entity; or • for important public interest reasons. You must inform individuals when you decide to lift a restriction on processing. **All requests must be passed immediately to the DPO.**
Right to data portability **This includes the right to:** • **receive a copy of the personal data, free of charge, from the data controller in a commonly used and machine-readable format and store it for further personal use on a private device;** • **transmit the personal data to another data controller; and** • **have personal data transmitted directly from one data controller to another where technically possible.**	The right to data portability only applies: • to personal data that an individual has provided to a controller; • where the processing is based on the individual's consent or for the performance of a contract; and • when processing is carried out by automated means. We must respond without undue delay and within one month or, if the request is complex or there are numerous requests, this can be extended by two months. We must inform the individual of any extension within one month of the receipt of the request and explain why it is necessary. If we are not taking any action, we must explain why to the individual, without undue delay and within one month, informing them of their right to complain to the supervisory authority and to a judicial remedy. **All requests must be passed immediately to the DPO.**
Right to object **Individuals have the right to object to:** • **processing based on legitimate interests or the performance of a task in the public**	If processing for the performance of a legal task or legitimate interests, individuals must have an objection on "grounds relating to his or her particular situation". We must stop processing the personal data unless: • we can demonstrate compelling legitimate grounds for processing, which override the interests, rights and freedoms of the individual; or

Right provided by GDPR	Notes
interest/exercise of official authority (including profiling); • **direct marketing (including profiling); and** • **processing for purposes of scientific/historical research and statistics.**	• the processing is for the establishment, exercise or defence of legal claims. If processing for the performance of a legal task or legitimate interests or for direct marketing purposes: • We must inform individuals of their right to object "at the point of first communication" and in the privacy notice. • This must be "explicitly brought to the attention of the data subject and presented clearly and separately from any other information". If processing for direct marketing purposes, there are no exemptions or grounds to refuse. If we receive an objection to processing for direct marketing purposes: • we must stop processing personal data for direct marketing on receipt; and • we must deal the objection at any time and free of charge. If processing for research purposes, individuals must have "grounds relating to his or her particular situation" in order to object. We are not required to comply with an objection if we are conducting research where the processing of personal data is necessary for the performance of a public interest task. If our processing activities fall into any of the specified categories and are carried out online, we must offer a way for individuals to object online. **All requests must be passed immediately to the DPO.**
Rights in relation to automated decision making and profiling **Individuals have the right not to be subject to a decision when:** • **it is based on automated processing; and** • **it produces a legal effect or a similarly significant effect on the individual.**	The right does not apply if the decision: • is necessary for entering into or performance of a contract between us and the individual; • is authorised by law (eg for the purposes of fraud or tax evasion prevention); • is based on explicit consent; or • does not have a legal or similarly significant effect on the individual. We must ensure that individuals are able to: • obtain human intervention; • express their point of view; and • obtain an explanation of the decision and challenge it. **All requests must be passed immediately to the DPO.**

APPENDIX B: Data Protection Impact Assessment (DPIA)

Primary contacts for advice and guidance:

Kerry Jenkins
Data Protection Officer
Interim Director of Resources
TEDI-London
dpo@tedi-london.ac.uk
020 3813 0126

David Minahan
Chief Information Officer
IT Services
TEDI-London
c/o dpo@tedi-london.ac.uk
020 3813 0147

Summary

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project or process.

You must conduct a DPIA for processing that is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

You should fill out the DPIA at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan. Further Information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Screening questions

These questions are intended to help you decide whether a DPIA is necessary. **Answering 'yes' to any of these questions is an indication that a DPIA is required**. You can expand on your answers as the project / process develops if you need to.

1. Will the project / process involve the collection of new information about individuals?

2. Will the project / process compel individuals to provide information about themselves?

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

5. Does the project / process involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

6. Will the project / process result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

8. Will the project / process require you to contact individuals in ways that they may find intrusive

Submitting controller details

Name of controller	TEDI-London
Title of DPO	Director of Resources
Name of DPO	Nancy Huggett

Step 1: Identify the need for a DPIA

Explain broadly what 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.

Step 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 other 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?

The GDPR defines special category data as:

- *personal data revealing **racial or ethnic origin**;*
- *personal data revealing **political opinions**;*
- *personal data revealing **religious or philosophical beliefs**;*
- *personal data revealing **trade union membership**;*
- ***genetic data**;*
- ***biometric data** (where used for identification purposes);*
- *data concerning **health**;*
- *data concerning a person's **sex life**; and*
- *data concerning a person's **sexual orientation**.*

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply. For further information, please see our separate guidance on criminal offence data.

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?

Step 3: 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?

Step 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?
The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data: ***(a) Consent:*** *the individual has given clear consent for you to process their personal data for a specific purpose.* ***(b) Contract:*** *the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.* ***(c) Legal obligation:*** *the processing is necessary for you to comply with the law (not including contractual obligations).* ***(d) Vital interests:*** *the processing is necessary to protect someone's life.* *(e)* ***Public task****: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.* *(f)* ***Legitimate interests:*** *the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)*

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

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 accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/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 kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX C: Personal Data Breach Reporting Form and Examples

Actual and suspected personal data breaches should be reported using the form below. Examples of persona data breaches are listed below. It you are in doubt, make a report.

Human error

- Personal data emailed, posted or handed to the wrong recipient
- Excessive/non-essential personal data provided to otherwise valid recipients
- Personal data received in error
- Loss of hard copy material containing personal data
- Loss of any TEDI-London data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device (NOTE: Loss of any privately-owned devices should only be reported if they contain personal data related to university activities)
- Unauthorised publication of personal data onto a website or social media channel

Theft

- Theft of hard copy material containing personal data
- Theft of any TEDI-London data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device (NOTE: Theft of any privately-owned devices should only be reported if they contain personal data related to university activities)

Malicious intent

- Attempts (either failed or successful) to gain unauthorised access to university systems, e.g. hacking
- Virus or other malicious malware attacks (suspected or actual)
- Compromised user accounts, e.g. disclosure of user login details through phishing
- Information obtained by deception ("blagging")
- Deliberate leaking of personal data

Malfunctions

- Failure of software or hardware leading to personal data loss
- Damage or loss of personal data due to fire, flood, power surge or other physical damage

Personal Data Breach Reporting Form

This form should be completed by a TEDI-London staff member who experiences, or discovers a data breach, or their line manager, and sent to the Data Protection Officer (dpo@tedi-london.ac.uk) and, where IT related, the Chief Information Officer as soon as possible following discovery of the incident.

Please send the form even if you cannot complete all the questions as any missing answers can be provided as and when the information becomes available. Please note that circulation of this form and any related documents must be restricted to those directly involved in investigating the incident and that no data subjects should be referred to by name in this report.

Your details	
Name and role title	
Email	
Telephone	
Date of Report	
Details of the data breach: Questions in **BOLD** must be answered	
Time and date breach was identified and by whom	
Description of incident – include time, date, location, how the incident occurred etc	
If there has been a delay in reporting this incident please explain why	
Details of any third-party service providers involved in the breach	
What measures were in place to prevent an incident of this nature occurring (e.g. encryption, back-ups, procedures, training)	
Please provide extracts/links to any policies and procedures considered relevant to this incident	
Personal Data Compromised: Questions in **BOLD** must be answered	
Type of personal data compromised (please provide examples and/or as much detail as possible)	
Sensitive personal data compromised (specify which, if any) Sensitive personal data = race/ethnicity, political/religious beliefs, Trade Union membership, physical/mental health or condition, sexuality/sex life, criminal offence, genetic data, biometric data where processed to uniquely identify an individual. For the purposes of data breach management, other information such as bank account details should also be classed as sensitive due to the risk of fraud.	

Potential adverse consequences for the individuals – what are they, how serious or substantial are they and how likely are they to occur?	
Number of individuals whose personal data has been compromised	
Volume of data/records involved	
Type of individuals whose data has been compromised (e.g. students, staff, alumni, community / industry partners, job applicants etc)	
Are the affected individuals aware that the incident has occurred?	
Have any affected individuals complained about the incident?	
Incident Management: Containment and Recovery: Questions in **BOLD** must be answered	
Is the breach contained or ongoing?	
What steps were/will be taken to contain the breach?	
When was the breach contained?	
If data lost or stolen, what steps are being taken to recover the data? If already recovered, when was the data recovered?	
Who has been informed of the breach (both inside and outside of TEDI-London)	
Details of regulatory bodies or collaborative partners who may need to be informed	
Has there been any media coverage of the incident? If so provide details	
Training and Prevention of Incident Re-occurring	
Has the person(s) responsible for or involved with the breach completed TEDI-London's Data Protection flick learning training? If so, when was this completed?	
What steps can be taken to minimise the possibility of a repeat of such an incident?	
To be completed by the Data Protection Officer	
Overall assessment of incident: (a) no risk to the data subject; (b) risk* to the data subject; or (c) high risk** to the data subject? Provide brief explanation for decision. *Risk = must notify ICO **High risk = must notify data subject	