Data Protection and Privacy Policy

Title:	Data Protection Policy and Privacy Policy
Owner:	Information Governance Office
Approved By:	TU Dublin GDPR Steering Group
Approval Date:	December 2018
Next Review Date:	December 2019

Chapter 1. Introduction

1.1. Background

The General Data Protection Regulation ('GDPR') came into force on 25th May 2016 and organisations must implement it by 25th May 2018. It replaces Directive 95/46/EC with the aim of harmonising EU data protection law. The new law introduces a range of requirements that have significant impact on organisations including, but not limited to mandated organisational accountability with a heavy focus on implementing robust privacy governance frameworks; privacy impact assessments; privacy by design; data breach notification; and a stronger focus on the rights of a data subject. Enforcement fines for non-compliance can be as high as €20 million or 4% of annual turnover, whichever is larger.

TU Dublin is committed to ensuring the privacy rights of individuals are upheld at all times. The purpose of this Data Protection Policy ('DP Policy') is to define TU Dublin – City Campus standards for managing personal data, outlining the key principles that must be followed to ensure the appropriate collection, use and protection of personal data and how TU Dublin – City Campus complies with Data Protection legislation.

As part of our mission we are required to collect, use and keep personal data (information) about its staff, students and other individuals who come in contact with the University in accordance with the requirements outlined in the GDPR.

The purposes of processing this data by TU Dublin – City Campus include the organisation and administration of courses, research activities, the recruitment and payment of staff, compliance with statutory obligations and compliance with legal obligations to funding bodies and government, etc. To comply with the relevant legislation, data about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully by TU Dublin – City Campus. All documents created and received by the TU Dublin in the course of its official business (including teaching, research and administration), and the Technological Universities Act 2018, constitute the official records of TU Dublin – City Campus.

Records Management is the application of systematic control over information which is required in the administration and operation of TU Dublin – City Campus activities. The information that we record contain serves as evidence of functions executed and activities performed and comprise a valuable source of knowledge as to how and why decisions were taken. Records created or received by TU Dublin – City Campus staff in the course of their duties on behalf of TU Dublin – City Campus , can be in a variety of physical forms including: paper documents including both written and printed matter, books, drawings, electronic data on any media, photographs, or anything on which information is recorded or stored by graphic, electronic or mechanical means, or copies thereof received by an academic or administrative office of TU Dublin – City Campus in connection with the transaction of TU Dublin – City Campus business and retained by such office as evidence of the activities of TU Dublin – City Campus or because of the information contained therein.

In addition, it is worth noting that Freedom of Information (FOI) has since its introduction in 1998 made a major contribution to facilitating access by citizens to official information. It has contributed to a shift towards greater openness and transparency in the conduct of official activities and in Ireland's administrative and political culture. FOI requests are made and responses are sought in various formats and there are legal complexities in the interaction with other legislation such as the GDPR and other access to information regimes. It is important that a strong framework must be in place within each public body to support the effective implementation of the FOI Act 2014. The structures put in place in each public body are pivotal to the effective performance of the public body in relation to delivering on their commitment to quality in meeting their obligations under FOI as well as minimising the administrative burden of FOI. The details of these are contained in a separate Freedom of Information Policy of TU Dublin – City Campus.

1.2. Purpose of this Policy

The purpose of this overarching Data Protection Policy is to detail a statement of TU Dublin – City Campus's commitment to protect the rights and privacy of individuals in accordance with the GDPR, to set out requirements to collection, use, transfer and destruction of personal data processed by TU

Dublin – City Campus, and to outline principles for the classification, handling and administration of the data of TU Dublin – City Campus in that regard.

Data Protection Policy (DP Policy) consists of the following supporting policies which form integral part of the DP policy:

Policy	**Summary**	**Section**
Data Retention Policy	This sets out how TU Dublin – City Campus will safeguard and retain personal data in compliance with the "storage limitation" principle. This policy also outlines the accepted purging and destruction methods for personal data.	Chapter 3
Data Breach Policy	This sets out TU Dublin – City Campus policy regarding classification, reporting, notification and documentation of personal data breaches in compliance with the 'integrity and confidentiality' principle.	Chapter 4
Data Subject Rights Policy	This sets out TU Dublin – City Campus's policy regarding data subject rights requests from individuals.	Chapter 5
Privacy by Design and Data Protection Impact Assessments Policy	This policy describes how TU Dublin – City Campus meets its obligations to individuals, and legal and regulatory requirements, regarding the safeguarding of personal data through the implementation of Privacy by Design. The policy also describes the process by which TU Dublin – City Campus assesses the data protection risks in any new projects.	Chapter 6
Records of Processing Policy	This policy TU Dublin – City Campus's policy regarding documentation and maintenance of records of processing activities to comply with 'accountability' principle.	Chapter 7
Direct Marketing Policy	This policy describes how TU Dublin – City Campus meets its obligations to individuals and its legal and regulatory requirements, regarding direct marketing procedures, to be compliant with the GDPR and the e-Privacy Directive.	Chapter 8
Data Processor Management and Data Transfer Policy	This policy describes how TU Dublin – City Campus meets its obligations to individuals, and legal and regulatory requirements regarding data sharing relationships whether this involves one-off or systematic disclosures. Also, this policy describes the due diligence guidelines that should be adopted by all business areas across TU Dublin – City Campus when selecting data processors that will engage in carrying out certain services to TU Dublin – City Campus.	Chapter 9

1.3. Key Definitions:

For the purposes of this Policy:

"Data Subject" means an individual who is the subject of personal data. **"Natural person**" is a living individual. Although other laws may apply, the GDPR does not apply to deceased persons.

"**Personal data**" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular reference to 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 natural person.

"**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not, by automated means, such as collection, recording, organisation structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction erasure or destruction.

"**Special categories data**" (sensitive personal data) means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural persona, data concerning health or data concerning a natural person's sex life or sexual orientation.

Further definitions can be found in **Appendix 1** of this document.

1.4. Scope and Applicability

This policy applies to all areas and locations of TU Dublin – City Campus and includes all departments, offices, units, research centres and areas of work, which form part of the institutional structure. This policy is equally applicable to records created and preserved in both paper and electronic format. This Policy also applies to individuals who are not directly employed by the University, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the University as well as University clubs and societies.

All TU Dublin – City Campus employees, students and relevant third parties who process data on the University's behalf must apply standard set out in the DP policy when dealing with personal data of data subjects in their areas. Data subject whose data TU Dublin – City Campus processes can include the following categories:

- Employees, including full time, part time, permanent and temporary employees.
- Students, including existing undergraduate, postgraduate, research students who are completing full time or part time studies, apprentices, referred or exchange students. This category also include prospective students who expressed interested in the programmes provided by TU Dublin – City Campus.
- Children are natural persons under age of 16.
- General population are natural persons who are not employees or students of TU Dublin – City Campus but have come into contract with TU Dublin – City Campus through a number of Functional Areas within the University. For example, but not limited to, patients, sponsors, donors, and visitors.

This Policy outlines the minimum standards of how to adhere to these rules and obligations.

1.5. Monitoring and Compliance

All staff, students, third parties and any other person who processes on behalf of TU Dublin – City Campus is required to adhere to the requirements set out in this DP Policy. Failure to comply with the DP Policy and related data protection policies referenced in this document will be regarded as a significant breach of our obligations under the GDPR, and could result in a breach of the data protection legislation. For the avoidance of doubt, whether personal data is obtained directly from an individual or obtained through the fulfilment of a process with another Functional Area or a third party, it is the responsibility of all Functional Areas that process personal data to ensure compliance with the minimum standards outlined in this Policy.

Failure to comply with this policy may lead to disciplinary action, up to and including dismissal in the case of staff, expulsion in the case of students, being taken in accordance with the University's disciplinary procedures. Failure of a third party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the Information Governance Officer and Data Protection Officer (IGO and DPO) in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

1.6. Status of this Policy

This Policy has been approved by the Universities GDPR Steering Group and applies to all staff and students of the University and other individuals who come into contact with TU Dublin – City Campus.

If you have any queries or require clarification on any aspect of Data Protection, please contact:

The Information Governance Officer and Data Protection Officer

Information Governance Office
Technological University Dublin
5th Floor Park House Grangegorman
191 North Circular Road
Dublin 7
D07 EWV4

Email: foi@dit.ie
Tel: 353 1 2205027

Review of this Policy

This Policy will be reviewed annually in light of any legislative changes or other relevant changes in TU Dublin – City Campus's processing environment.

Chapter 2. Data Protection Principles

2.1. Data Protection Policy

This Data Protection Policy stems from the rights and responsibilities in relation to the principles, classification, handling and administration of personal data, and these are detailed in the following sections.

2.1.1. Data Protection Principles

The data protection principles as outlined in the GDPR are a set of requirements, which the Functional Areas have to follow when processing personal data. The principles require that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) Accurate and, where necessary, kept up to date.

(e) Kept for no longer than necessary.

(f) Processed in a manner that ensures appropriate security of the personal data.

(g) Be able to demonstrate compliance with the principles.

Appendix 1 describes each principle in detail and should be read in full.

2.1.2. Enforcing data subjects rights

The GDPR provides individuals with a number of rights in relation to their personal data including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- The rights in relation to automated decision making and profiling.

Functional Areas that process personal data are required to have procedures in place to be able to enforce data subject rights with respect to each of the rights listed above.

All data subject rights have to be processed in accordance with the requirements and statutory timeframes laid down by the GDPR.

In order to processes individuals' personal data in transparent manner, Functional Areas have to provide data subjects a notice or statement when collecting their data that detail the following:

- identity and contact details of the controller and contact details of the IGO and DPO;

- purposes for the processing and legal basis for processing including legitimate interests of the controller;
- recipients or categories of recipients;
- details of data transfers outside of the EU and the measures of protection including how the individual can obtain a copy of the safeguards used;
- retention periods for the data;
- individuals rights to complain to a supervisory authority;
- Any automated decision making including the logic involved and the significance and consequences of the processing for the individual.

Consultations should be sought with IGO and DPO if necessary. Refer to **Data Subject Rights Policy** in **Chapter 5** for further detailed requirements on responding to data subject rights requests.

2.1.3. Personal data breach notification

TU Dublin – City Campus as a data controller is a legally required to notify the Office of Data Protection Commissioner where a personal data breach is likely to result in a risk to data subjects' rights and freedoms.

In addition, Functional Areas are legally required to notify affected individuals (data subjects) where a personal data breach is likely to result in a high risk to their rights and freedoms. For further guidance on what constitutes a high risk, please see the TU Dublin – City Campus Data Breach Policy.

TU Dublin – City Campus is required to notify the Data Protection Commissioner within 72 hours after having become aware of the personal breach. Therefore, Functional Areas have to implement robust processes and procedures in place to identify and report suspected personal data breach incidents. These procedures should also cover errors and "near misses".

Functional Areas also have to implement an internal reporting procedure. This has to include documentation of any suspected personal data breach, comprising the facts relating to the breach, its effects and the remedial action taken. Failure to report a notifiable breach could result in enforcement action by the Data Protection Commissioner including the imposition of an administrative fine of up to €10,000,000 or 2% total worldwide annual turnover.

Refer to **Data Breach Policy** in **Chapter 4** for detailed requirements on reporting data breaches.

2.1.4. Transfer and Sharing of data

As part of its legal obligations TU Dublin – City Campus transfer and share personal data within the University and to third parties which are external to TU Dublin – City Campus. In order to fulfil TU Dublin – City Campus's legal obligation without jeopardising rights and freedoms of individuals, the Functional Areas have to ensure:

- Contracts and/or data processing agreements are in place when personal data is transferred to an external third party.
- When personal data is transferred within TU Dublin – City Campus, it is documented in internal policy, procedures and processes.
- Transfer of personal data is carried out in a secure manner (e.g. encrypted and password protected files).
- Data minimisation principle is applied when transferring personal data.
- All transfers have to be reflected in records of processing activities, and updated when any changes occur.

In addition, the GDPR imposes restrictions on the transfer of personal data outside the European Economic Area (EEA), to third countries or international organisations in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Therefore, Functional Areas must not transfer personal data outside the EEA unless that country ensures an adequate level of protection. Functional Areas (or third parties) intending to process personal data outside the EEA should consul legal advisor to ensure adequate contractual clauses are implemented.

Refer to **Data Processor Management and Data Transfer Policy** in **Chapter 9** for detailed requirements for data transfer and sharing.

2.1.5. Data protection by design and by default

TU Dublin – City Campus has a general obligation to implement technical and organisational measures to show that TU Dublin – City Campus has considered and integrated data protection into our processing activities. Data protection by design and by default is an approach to projects that promotes privacy and data protection compliance from the start. “Projects” which would benefit for data protection by design approaches include, (but are not limited to) building new IT systems for storing/accessing personal data; developing strategies/services that have privacy implications; using personal data for new purposes.

Data protection by design tools can include data minimisation, pseudonymisation, and the use of Data Protection Impact Assessments.

Functional Areas should implement a procedure as to what measures they can adopt to meet the principle of data protection by design and by default.

Refer to **Privacy by Design and Data Protection Impact Assessments Policy** in **Chapter 6** for detailed requirements.

2.1.6. Data Protection Impact Assessments

Data Protection Impact Assessment (DPIA) is a tool which can help the Functional Areas to identify the most effective way to comply with its data protection obligations and meet individuals’ expectation of privacy, and in turn, allow it to fix problems in the early stages of a project.

Functional Areas have to carry out a DPIA when:

- The processing is likely to result in a high risk to the rights and freedoms of individuals.
- Using new technologies, for example, use of fingerprint or facial recognition for physical access control.

A DPIA should contain at minimum the following:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by TU Dublin – City Campus.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures envisaged to address the risks.

Functional Areas should identify and assess where DPIAs would be required within the context of their processing activities.

Refer to **Privacy by Design and Data Protection Impact Assessments Policy** in **Chapter 6** for detailed requirements.

2.1.7. Management of Data Processors

Where TU Dublin – City Campus engages a third party to process personal data on its behalf, the GDPR places specific obligations on TU Dublin – City Campus. These third parties are known as 'data processors'. In order to demonstrate compliance in managing data processors, Functional Areas should ensure:

- Prior to engaging a data processor, adequate due diligence is carried out to ensure that the data processor have suitable data protection practices and framework in place.
- Following this, any such processing must be subject to a contract between the Functional Areas and the third party.
- Right to audit clauses contained within contracts should be utilised in order for TU Dublin – City Campus to verify that data processors are compliant with the University's requirements to data protection.
- Where TU Dublin – City Campus is entering joint controller arrangements with another data controller, Functional Areas have to ensure that appropriate governance arrangements are in place, stipulating the roles and responsibilities of each data controller.

Refer to **Data Processor Management and Data Transfer Policy** in **Chapter 9** for further details on the management of relationships with data processors.

2.1.8. Demonstrating Accountability

In order for TU Dublin – City Campus to demonstrate compliance with the Data Protection Principles, the Functional Areas have to put in place comprehensive governance measures. In addition, to the requirements set out in section 2.1. (g) of this Policy, the GDPR requires:

- The Functional Areas to maintain records of its processing activities, which it must also provide to the Data Protection Commissioner upon request.
- Further information regarding maintaining these records can be found in the **Record of Processing Policy** in **Chapter 7**.
- Functional Areas should ensure that they have implemented and documented procedures and processes to comply with each of the minimum requirements outlined in this Policy.

2.1.9. Direct Marketing

Some Functional Areas are engaged in direct marketing activities, and contact individuals, including students, employees or general population, with promotional materials. When individuals are contracted for direct marketing purposed, the Functional Areas have to ensure the following:

- Consent to directly market to individuals is obtained prior to using their personal data, and this consent meet the standard of consent required by the GDPR, which is that consent should be freely given, unambiguous, and worded in a plain easy to understand language.
- Where engaged in direct marketing activity, Functional Areas must have put procedures in place to ensure individuals are only communicated with in line with their direct marketing consent, and comply with other relevant legislation for contacting individuals, for example, ePrivacy Regulation.

2.2. Data Classification and Data Handling

The University as a public organisation subject to FOI has the following four classifications of Data:

- Private data,
- Public data,

- Sensitive Personal data and
- Personal data.

Each category of data requires a different form of security or protection based on its classification and a risk in case of a potential data breach or the strategic impact to the University if the security of that data was compromised.

The University in addition to the classifications above has a data handling policy that sets out the manner in which the various types or classes of data set out in the data classification should be managed across the data flow lifecycle i.e. from collection, storage, transmission, processing to destruction.

Refer to Table 1 below for detailed requirements.

Table 1. Data Classification and Data Handling Responsibilities

Data Classification	Description	Data Owner & Decision Maker	Data handling Responsibilities				
			Collection	**Storage**	**Transmission**	**Processing**	**Destruction**
Public Non - Personal Data	TU Dublin information which is not prohibited by law to publish.	Head of Function	N/A	N/A	By the appropriate Head of Function	N/A	N/A
Private Non - Personal Data	TU Dublin information which is subject to a confidentiality agreement, or the concerns financial, commercial, or intellectual property matters the disclosure of which would cause material loss.	Head of Function	As authorised by the Appropriate Head of Function.	• Physical documents subject to physical security in locked storage. • Computer data subject to IS security password or encryption.	• Physical documents transmitted with physical security measures, by informed employees, or courier firms with confidentiality agreements with TU Dublin – City Campus. • Computer data only emailed subject to IS security or encryption.	• On the authority of the appropriate Head of Function. • By third parties on the authority of the appropriate Head of Function, and subject to a confidentiality agreement.	• Data is destroyed on Authorisation of Head of Function. • Function's Data or Records Retention Schedule is updated on destruction
Personal Data	TU Dublin data relating to a living individual who may be identified from the data.	Head of Function	• Collected based on a lawful ground for the specified and defined	• Subject to appropriate physical locked storage and IS security	• Data is transmitted only as necessary for the purpose it was collected. Transfer to countries outside EEA and approved	• Data is processed only in ways compatible for the purpose for which it was initially collected.	• Data stored in all formats is destroyed on Authorisation n of Head of Function when

Data Classification	Description	Data Owner & Decision Maker	Data handling Responsibilities				
			Collection	**Storage**	**Transmission**	**Processing**	**Destruction**
Sensitive Personal Data	TU Dublin – City Campus special category of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; criminal convictions or the alleged commission of an offence; personal data of a financial nature.	Head of Function	purpose. • Ensure data collected is adequate, relevant, not excessive, and retained no longer than necessary for the specified purpose. • Ensure that privacy statement is provided at the time of collection or initial contact with individual.	password or encryption. • Subject to Data Subject Rights . • Subject to being kept accurate and up to date. • Subject to minimisation and retention for no longer than is necessary for the specified purpose.	countries by the European Commission should be governed by a contract. Transfer outside EEA has to be added to privacy notices. • Physical documents transmitted with physical security measures, by informed employees, or courier firms having confidentiality agreements with TU Dublin – City Campus. • Computer data only emailed subject to IS security password or encryption.	• On the authority of the appropriate Head of Function. • By third parties on the authority of the appropriate Head of Function, and subject to contracts, a confidentiality agreement. And data processing agreements. • Consent is required to processes for new purposes. Subject to derogations under the GDPR.	its purpose is fulfilled. Subject to legal obligations. • Function's Data or Records Retention Schedule is updated on destruction.

2.3. Roles and Responsibilities

TU Dublin – City Campus through the President and the Senior Leadership Team has overall responsibility for ensuring compliance with the GDPR and this Policy. However, all employees (where they are employed) or students (in the course of their studies) of the University, and third parties, who collect and / or control the contents and use of personal data on behalf of TU Dublin – City Campus, are also responsible for compliance with the GDPR and this Policy.

2.3.1. Role of the Operation & Resources Committee and the GDPR Steering Group

The Operations & Resources Committee (ORC) is responsible for the internal control of TU Dublin – City Campus, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. The TU Dublin – City Campus GDPR Steering Group is a sub-committee of the ORC, and is responsible for:

- Reviewing and approving this Policy and any updates to it as recommended by the Information Governance Office;
- Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.

2.3.2. Role of the Information Governance Officer and Data Protection Officer

The University has appointed an Information Governance Officer and Data Protection Officer in the Information Governance Office who will assist the University and its staff with compliance with the GDPR and the FOI Act. The contact details of the IGO and DPO are listed in **section 1.6**.

The President has designated the Information Governance Officer as the IGO and DPO to assist the University and its staff in compliance with the General Data Protection Regulations (GDPR).

The DPO is the Senior Officer within the University responsible for statutory compliance with the GDPR and has the following tasks:

- To inform and advise TU Dublin – City Campus staff and students, or third parties who carry out processing of personal data on behalf of TU Dublin – City Campus of their obligations under the GDPR, the Data Protection Act 2018, and to other data protection provisions;
- To monitor compliance with the GDPR, the Data Protection Act 2018, with other data protection legislation and provisions, and with the TU Dublin – City Campus policies and procedures in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested in regards to the data protection impact assessments and monitor the compliance as required by the GDPR;
- To cooperate with the Office of Data Protection Commissioner, and to act as the contact point for the Office of Data Protection Commissioner on issues relating to data processing at TU Dublin – City Campus, and to consult, where appropriate, with regard to any other matter.

In addition, the DPO has the following responsibilities:

- Ensuring that this Policy is regularly reviewed and approved by the GDPR Steering Group as appropriate as well as ensuring documentation is updated as appropriate;
- Ensuring that procedures and guidelines are developed to support this Policy;
- Ensuring that any data security breaches are properly dealt with and liaising with the Office of the Data Protection Commissioner where necessary/appropriate;
- Processing and responding to formal Data Subject Access Requests while liaising with relevant Decision Makers in University departments/offices regarding such requests;

- Organising targeted training and briefing sessions for staff as required;
- Providing advice and guidance to staff on data protection matters;
- Maintaining a centrally-held register of the categories of personal data held by the University;
- Maintaining a list of nominated Decision Makers persons with responsibility for coordinating data protection matters within their own areas.

2.3.3. Role of Head of School / Function

It is the responsibility of each Director to designate each Head of Function as the owner of records in their area. Where records are used by more than one area, it is the responsibility of each area to ensure that the ownership of the record is agreed and established. Each Head of School / Function must ensure that the IGO and DPO is informed of any changes it uses of personal data that might affect TU Dublin – City Campus's compliance with the GDPR. It is the responsibility of the Head of School / Function to ensure that appropriate security measures are observed for maintaining records containing personal or other confidential information.

Every School and Function within the University, which processes personal data, is required to nominate a suitable member of staff to be responsible for coordinating Data Protection compliance matters within their respective area, such matters to include:

- Being a point of contact for the IGO and DPO regarding Data Protection;
- Bringing relevant Data Protection/IT data security matters to the attention of relevant staff in his/her area;
- Participating in training in data protection/IT data security where appropriate.

2.3.4. Role of Data Protection Commissioner

The Data Protection Commissioner is an Irish Data Protection Authority (or Supervisory Authority) which oversees national compliance with the terms of the GDPR and Data Protection Act. The Office of the Data Protection Commissioner (ODPC) has a wide range of enforcement powers, including investigation of University records and record-keeping practices. Summary proceedings for an offence under the GDPR may be brought and prosecuted by the ODPC.

The GDPR imposes certain responsibilities on the Data Protection Commissioner as the national Data Protection Authority, including but not limited to the following:

- Monitor and enforce the application of the GDPR;
- Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children receive specific attention;
- Promote the awareness of data controllers and data processors of their obligations under the GDPR;
- Upon request, provide information to any data subject concerning the exercise of their rights under the GDPR and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
- Handle complaints lodged by a data subject, or by a body, organisation or association and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
- Conduct investigations on the application of the GDPR, including on the basis of information received from another supervisory authority or other public authority;
- Establish and maintain a list in relation to the requirement for data protection impact assessment;

- Give advice on the processing operations;
- Keep internal records of infringements of the GDPR;
- Fulfil any other tasks related to the protection of personal data.

2.4. Training and Awareness

The University is committed to the provision of data protection training on a mandatory basis as well as necessary in addition to an opt-in basis to ensure all individuals are aware of their respective obligations under the GDPR. This is especially important for staff who handle personal data and / or sensitive personal data in the course of their everyday business.

To achieve this, the University will support the development, rollout and communication of Data Protection training and an awareness program across TU Dublin – City Campus. This program will ensure that staff are regularly reminded of data protection principles, requirements set out in data protection and related policies throughout the year, and not simply when a policy is updated.

In addition, on an annual basis, all employees are required to complete the mandatory on-line data protection refresher training. Training will require completion on a short assessment to evaluate the understanding of the Data Protection Principles, and TU Dublin – City Campus requirements.

Head of School / Function are required to ensure timely completion by their staff of mandatory on-line training and maintain records in relation to exceptions (e.g. due to extended leave) and manual completions. Where the Functional Areas identify a need for specific key, risk data protection training, records of such activity should be retained (i.e. content and attendance).

For electronic communications, confirmation of reading and tracking of responses will be put in place to ensure staff follow through on a commitment to be aware of the policies.

All sections, offices and staff are required to:

- Acquaint themselves with, and abide by, the Data Protection Principles set out in this Policy, and TU Dublin – City Campus Data Protection Guidance;
- Read and understand this policy document;
- Understand what is meant by ‘personal data’ and ‘sensitive personal data’ and know how to handle such data;
- Not jeopardise individuals’ rights or risk a contravention of the GDPR;
- Timely complete mandatory on-line data protection training;

Contact their Head of School / Function or IGO and DPO if in any doubt.

2.5. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories, which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of ICT where required.

2.6. Accountability and Record Keeping

The Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Chapter 3. Data Minimisation and Retention Policy

The purpose of this chapter is to outline the requirements for the management of TU Dublin – City Campus records processed by or on behalf of TU Dublin – City Campus. Key requirements for records management are:

- Retain all records (whether in paper, electronic or other recording medium) for the period required by, and to demonstrate compliance with, applicable laws;
- Retain records containing personal information for no longer than necessary, as may be required by applicable laws;
- Maintain adequate records for individuals who need access to them;
- Halt records destruction upon receipt of service of legal processes, for example subpoenas, regarding those records;
- Identifying and appropriately safeguarding records of value to TU Dublin – City Campus;
- Assure the privacy and security of certain types of records; and
- Retain those records necessary to retain essential corporate knowledge.

3.1. Creating a Records Retention Schedule

- The Head of Function is required to ensure that records / data retention schedules for records and data held in their area are created that define the length of time that specified types of records and data are to be retained as well as their final disposition and method of disposition.
- While the Head of Function may delegate this responsibility to a member of staff in their area, the Head is usually the officer responsible for the initial collection / input and use of the data and synonymous with the "record owner" or the "information owner."
- Retention schedules have to be based on a determination of **legal retention requirements** as defined in relevant statutes and regulations, **financial requirements**, **administrative requirements** and **operational requirements**.
- In considering how long to retain a record, Functional Areas have to consider data protection laws and regulation, the record's importance, the need for retention including the likelihood of need for future reference, ease of re-creating the record's contents from other sources, and the possible consequences of the record being unavailable in the future. The potential historical value of records is also a consideration.
- Each employee creating or maintaining a file, whether in paper or electronic format, is responsible in conjunction with their Head of Function for classifying that file for retention or destruction in accordance with this policy.
- Records Retention Schedules apply to both electronic and paper records held by TU Dublin – City Campus and in the absence of any electronic records management systems, staff are required to employ good housekeeping practices in the management of electronic documents, i.e. employ a naming convention, have a back-up schedule, delete regularly (especially e-mails), use passwords as appropriate, produce paper copies if required to maintain the integrity of manual files, etc.
- Electronic records should have the same retention schedules as their paper counterparts. In the case of electronic records, the Functional Areas, which created or maintains these records, have to formally agree back-up and recovery procedures with the TU Dublin – City Campus ICT Department.
- Following approval by the Head of Function, the schedules are to be forwarded to the IGO and DPO who will review and liaise with the relevant area on any queries.

- Once all queries have been resolved, the IGO and DPO will arrange for the retention schedules to be tabled for review and approval at the TU Dublin – City Campus GDPR Steering Group and subsequently noted at the TU Dublin – City Campus Operations and Resources Committee (ORC) prior to publication on the TU Dublin – City Campus website.

3.2. Reviewing a Records Retention Schedule

- The Head of Function is responsible for ensuring that reviews of retention schedules are carried out on a regular basis and in light of any legal or other relevant indicators. As a matter of good practice, at the very least, it should be re-assessed by the Head of Function after 3 years and sooner if the nature of the records changes in anyway.
- Changes to the retention schedules are to be advised directly to the IGO and DPO together with reasonable justification of the change, e.g. information on relevant legislation, policy changes, working practice changes etc.
- Once all queries have been resolved, the IGO and DPO will arrange for the retention schedules to be tabled for review and approval at the TU Dublin – City Campus GDPR Steering Group and subsequently noted at the TU Dublin – City Campus Operations and Resources Committee (ORC) prior to publication on the TU Dublin – City Campus website.

3.3. Disposition of Records / Data

- The Head of Function is required to establish a process to identify records that are expired and due for deletion. This process has to include frequency of processes operation (e.g. weekly, monthly, etc.). The processes should also include exceptions and halting procedures, where the records are required for investigations or legal claims, if this is applicable to the specific Functional Area. This might arise where TU Dublin – City Campus is subject to a request from a law enforcement or state security body to provide records, or where a record is required for the purposes of making or defending a legal claim. This should be in line with the processes.

- After the records and data have been retained for the requisite time set out in the retention schedules, the Head of Function is responsible for ensuring that these are either destroyed securely by means of secure shredding or stored for the requisite period or permanently in an appropriate TU Dublin – City Campus storage area utilising the Disposition of Records / Data Register.

- The final disposition (either destruction or transfer to storage) of records is carried out following review of the TU Dublin – City Campus Retention Schedules, as detailed in the Disposition of Records / Data Register Form in **Appendix 3.A**, after which time the records / data are either destroyed or transferred to TU Dublin – City Campus storage or Archives. Once completed these Disposition Forms will be circulated to and noted at the TU Dublin – City Campus GDPR Steering Group

- At the end of the relevant retention period all documents subject to this retention policy should be securely destroyed, which means deleting electronic files, discarding paper files in a manner consistent with the confidentiality of those files, and also deleting any back-ups. Records should be maintained of the document destruction process.

- Destruction of records shall take place only in compliance with this policy to avoid the inference that any record was destroyed in anticipation of a specific problem. Please note that TU Dublin – City Campus will treat seriously any destruction of documents before the retention period has elapsed and in particular destruction activity to avoid disclosing data that is subject to a legal requirement.

- If TU Dublin – City Campus records have to be retained for longer than prescribed in the Retention Schedules a risk assessment should be carried out by the Head of Function to identify whether this extension of the retention schedule can increase a risk to rights and freedoms of individuals, and can damage TU Dublin – City Campus in any way. Any decisions, with the input of the IGO and DPO that are made should be documented for future reference, and present for inspection when required.

3.4. TU Dublin – City Campus Records Retention Schedules

Within the University Record Retention Schedules are already in place and currently available in the following areas:

1. Academic Affairs and Quality Assurance
2. College & Schools
3. Estates
4. Financial Management & Accounting
5. Health and Safety
6. Technology Transfer Office – DRE
7. Human Resources - HR
8. Information Governance Office
9. Internal Audit
10. Information Services
11. Library Services
12. Property Legal Compliance
13. Payroll
14. Procurement
15. Public Affairs
16. Research, Enterprise, and Innovation Services
17. Student Affairs

3.5. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories, which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

3.6. Accountability and Record Keeping

Heads of Function are responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Appendix 3.A. Records / Data Retention Schedule Form: (Name of Function)

This schedule has been reviewed by the (**Insert Title of Head of Function**) in light of experience and any legal or other relevant indications as follows:

1.Records / Data Group	2.Records / Data Description	3.Data Classification	4.Records / Data Retention Period	5.Records / Data Rationale for Retention	6.Records / Data Final Disposition	7.Records / Data owner

1. **Records / Data Group:** Specify Records / Data Group e.g. Staff Files, Student exam results
2. **Records / Data Description:** Description of files e.g. Interview notes, minutes of meetings etc.
3. **Data Classification: See across***
4. **Records / Data Retention Period:** Length of time which records / data should be retained for
5. **Records / Data Rationale for retention:** Legal requirements as defined in relevant statutes and regulations, financial requirements, administrative requirements and operational requirements.
6. **Records / Data Final Disposition:** Action when records / data exceeds retention date i.e. archive or destroy confidentially
7. **Records / Data owner:** Position holder responsible for the records / data

*3 Data Classification	Description
Public Non – Personal Data	TU Dublin – City Campus Information which is not prohibited by law to publish
Private Non – Personal Data	TU Dublin – City Campus information which is subject to a confidentiality agreement, or the concerns financial, commercial, or intellectual property matters the disclosure of which would cause material loss.
Personal Data	TU Dublin – City Campus data relating to a living individual who may be identified from the data.
Sensitive Personal Data	TU Dublin – City Campus data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership, personal data of a financial nature.

Date Approved by Head of Function

Data Reviewed by Information Governance Officer and Data Protection Officer

Date Noted by SLT

Date of Last Review

Part I: Authorisation for Disposition of Records / Data

Appendix 3.B. Disposition of Records / Data Register Form

Function (Area / Office): _____ **Proposed Destruction Date**: _____

Record / Data Group	Records / Data Description	Volume of Records / Data	Disposition by Archive / Transfer / Destruction	Reason for Disposition

I certify that, as the relevant Head of Function, the above listed records / data may be disposed of in line with TU Dublin – City Campus's Record / Data Retention Schedule:

Signature: _____ **Date:** _____

Print name: _____ **Position:** _____

(Head of function)

Part II: Records / Data Destruction Certificate (*Please complete if records / data are to be destroyed)*

I certify that the above listed records / data were confidentially destroyed on _____ *(insert date of destruction)*

Signature: _____ **Date:** _____

Print name: _____ **Position:** _____

Chapter 4. Data Breach Policy

Data protection breaches can occur due to a variety of factors, impact different types of personal data and can lead to potential if not actual impacts to individuals. As such, each breach needs to be assessed on a case-by-case basis to determine the appropriate and necessary actions to take.

Each Functional Area is required to have processes in place for managing and investigating data breaches and near misses (potential data breaches).

4.1. Identification and Classification

Data breach can be identified through a variety of channels. For example:

- Customer or employee queries and/or complaints.
- Management of errors, as a result of the error itself or where the error may indicate a similar error in another area or processes.
- Control monitoring or internal quality checks.
- Assurance Reviews and Audits.

If a staff member considers that a data security breach has occurred, this must be reported immediately to the IGO and DPO at **foi@dit.ie** and relevant Line Manger by completing the **Personal Data Security Breach Report Form** in **Appendix 4.A** below.

ICT Services via the TU Dublin–City Campus Support Desk (phone 01 2205027 or email *support@dit.ie*) should also be advised of the potential breach.

The IGO and DPO will initially review the incident, as reported, and if a data security breach has occurred involving personal data or sensitive personal data they will liaise with the President who will decide if a Breach Management Group of relevant TU Dublin – City Campus stakeholders and a Chair should be appointed to investigate.

The Breach Management Group may include, amongst others as appropriate, the relevant Director or Head of Function, the Person reporting the incident, ICT Services, Public Affairs and the IGO and DPO. Any records relating directly to an investigation by the Breach Management Group will be retained by the IGO and DPO.

In order to comply with strict data breach notification requirements, an Emergency Breach Management Group will be held to make a decision on whether this breach is reportable to the ODPC and any affected individuals. The Emergency Breach Management Group have to consist of the relevant TU Dublin – City Campus stakeholders or the first point of contact, and will require to be available for the group meeting at a short notice.

4.2. Containment and Recovery

Containment involves limiting the scope and impact of a data security breach. If a breach has occurred, appropriate action will be taken by the relevant TU Dublin – City Campus stakeholders to minimise any associated risks, which may include:

- Establishing who within TU Dublin – City Campus needs to be made aware of the breach and ensuring relevant staff are informed what is required to assist in the containment exercise;
- Establishing whether there are any actions which may recover losses and limit the damage the breach can cause;
- Where appropriate, informing the Gardaí

4.3. Risk Assessment

In assessing the risk arising from a data security breach, the relevant TU Dublin – City Campus stakeholders require to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

4.4. Notification of Breaches

In accordance with the GDPR requirements, all incidents in which personal data has been put at risk must be reported to the ODPC within 72 hours of TU Dublin – City Campus becoming aware of the incident, including weekends.

The decision to report a breach to the ODPC will be made by the group of relevant TU Dublin – City Campus stakeholders investigating the incident.

However, if issues are raised relating to the adequacy of technological risk-mitigation measures, TU Dublin – City Campus will automatically report the incident to the ODPC.

If a decision is made by the group not to report a breach, a brief summary record of the incident with an explanation of the basis for not informing the ODPC will be retained by the IGO and DPO.

4.4.1. Reporting the data breach to the ODPC

If the group of relevant TU Dublin – City Campus stakeholders decided to report the data breach to the ODPC, the notification at minimum have to include the following information:

- Data breach description, including, if known, a description of the categories and a number of data subjects and of the personal data involved in the breach.
- A description of the likely consequences of the breach.

What measures TU Dublin – City Campus has taken to control and address the breach, including measures to mitigate the possible adverse effects for the affected individuals.

- The name and contact details of the IGO and DPO or other contact points within TU Dublin – City Campus that can answer questions, provide further information or address specific data protection concerns.

4.4.2. Reporting the data breach to the affected individuals

If the group of relevant TU Dublin – City Campus stakeholders decided to report the data breach to the affected individuals, the notification at minimum have to include the following information:

- Description of the data breach nature.
- A description of the likely consequences of the breach.
    - What measures TU Dublin – City Campus has taken to control and address the breach, including measure to mitigate the possible adverse effects for the affected individuals.
    - What TU Dublin – City Campus will do to assist individuals, and what steps the individuals can take to avoid or reduce the risk of harm or to further protect them e.g. change password.
- The name and contact details of the IGO and DPO or other contact points within TU Dublin – City Campus that can answer questions, provide further information or address specific data protection concerns.

4.5. Evaluation and Response

Subsequent to a data security breach, a review of the incident by the relevant TU Dublin – City Campus stakeholders will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Subsequent to each data, security breach a log will also be maintained by the IGO and DPO of the agreed steps arising from each incident and this will be presented by way of an overall annual report to the President or his nominated Committee.

4.6. Accountability and record keeping

Regardless of whether the data breach constitutes a personal data breach, the IGO and DPO must register all reported data breached and keep documentation. This is linked to the accountability principle contained in the GDPR. This register should contain a reasoning for the decisions taken in response to the breach, including a justification for not reporting a breach.

Failure to properly document a breach could lead to the ODPC taking enforcement action against TU Dublin – City Campus, including the imposition of administrative fines.

4.7. Training and Awareness

Functional areas should ensure that employees are made aware of, and understand the importance of data breach reporting requirements. This obligation also extends to any third parties / outsourced service providers, where they process personal data on behalf of TU Dublin – City Campus. Requirements should be incorporated relevant local procedures and training.

For further information on training and awareness, refer to **Data Protection Policy** in **Chapter 2.**

4.8. Third Parties / Outsourced Service Providers

Where processing of personal data is completed by a third party on TU Dublin – City Campus's behalf, Functional Areas are required to ensure it is undertaken in compliance with the GDPR and other related statutory requirements and have procedures in place to monitor compliance.

Any such processing must be subject to a contract between TU Dublin – City Campus (Data Controller) and the third party (Data Processor) which specifies the conditions under which the data can be processed, the security conditions attaching to the processing of the data and that the data will be deleted or returned upon completion or termination of the contract.

In these situations, TU Dublin – City Campus retains overall responsibility for the protection of personal data, but the third party (data processor) has an important role to play to enable TU Dublin – City Campus to comply with its obligations; and this includes breach notification. Data Processors are legally required to alert TU Dublin – City Campus of a personal data breach immediately.

Functional Areas have to ensure the third parties are aware of their obligations to report data breaches to the Functional Areas responsible for managing the third party. Specific conditions relating to the requirement for the third party to notify TU Dublin – City Campus of a personal data breach, have to be included in contractual agreements, subject to governance with the third party and included in assurance monitoring, audits or assessments of the third party.

Refer to **Data Processor Management and Data Transfer Policy** in **Chapter 9** for further details to what details should be outlines in the contractual agreements with data processors.

4.9. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

4.10. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Appendix 4.A. Personal Data Security Breach Report Form

As a matter of urgency when a Personal Data security breach has occurred please complete this form and return it to the IGO and DPO at **foi@dit.ie** and your Line Manger.

The requirement in Stage 4 above that all incidents in which personal data has been put at risk must be reported to the ODPC within 2 days of TU Dublin – City Campus becoming aware of the incident is relevant here.

1. Details of the data breach
2. Date and time incident occurred
3. Date and time incident detected
4. What type of data is involved?
5. Does data fall under the definitions of personal data and / or sensitive personal data outlined in Section 3?
6. Details on how the personal data was held (e.g. laptop, memory stick, personal digital assistant etc.)
7. Details of safeguards if any that would mitigate the risk if personal data has been lost or stolen. (e.g. encryption)
8. Are there any reasons to suspect that the passwords used to protect the personal data may have been compromised? (e.g. password stored with mobile device or weak password used)
9. Details of the number of individuals whose personal data is at risk (i.e. how many data subjects are affected by the breach?)
10. Details of those whose personal data has been breached (e.g. staff, students, suppliers or third parties)
11. Details of what the personal data could tell a third party about the data subjects affected
12. Any other relevant information or details that you consider relevant

Signed: _____ **Date:** _____

Chapter 5. Data Subject Rights Policy

A data subject (e.g. student, employee etc.) has certain rights in relation to the personal data that TU Dublin – City Campus holds on them. These rights include:

- Right to rectification;
- Right of access;
- Right to erasure;
- Right to restrict processing;
- Right to object;
- Rights in relation to automated decision making including profiling; and
- Right to data portability.

TU Dublin – City Campus has the following responsibilities in relation to data subject rights:

- To process requests in accordance with the GDPR.
- To have in place documented procedures in relation to each of the data subject rights.
- To maintain a log of all requests received and fulfilled, including where a request is refused and the justification for doing so.
- To comply with all requests within the regulatory timeframes.

5.1. Approach to Management of Data Subject Rights

In order to effectively manage data subjects' requests TU Dublin – City Campus will be required to ensure the following:

- Process requests in accordance with and specified by relevant legislation.
- Have in place documented procedures in relation to the data subject rights, which details the reporting structure.
- Comply with all requests within the regulatory timeframes. These timeframes have to be included in the internal data subject rights procedures.
- If TU Dublin – City Campus has disclosed the personal data in question to third parties, the University must inform them about the data subjects' request, unless it is impossible or involves disproportionate effort to do so. In considering whether this would be a disproportionate effort, TU Dublin – City Campus are required to determine the impact that this would have on the University's resources. TU Dublin – City Campus is also required to ensure that this is considered on a case-by-case basis. Where TU Dublin – City Campus decides that it would involve a disproportionate effort, it must document the justification for this.
- If TU Dublin – City Campus cannot comply with the data subjects' request, the University is required to communicate this to the individual. The communication has to include the reasoning, and inform the individuals of their right to complain to the ODPC, or their right to seek a judicial remedy.

The IGO and DPO will centrally manage all requests in conjunction with the Functional Areas and maintain a log of all requests received and fulfilled by the University, including where a request is refused and the justification for refusal decision. The data subject requests log can be requested by the Data Protection Commissioner for audit. The IGO and DPO is required to provide this log for inspection without undue delay.

A procedure to process data subject requests is detailed in **Appendix 5.B**.

5.2. Right to Rectification

The right to rectification is a data subject's right to have their information corrected where it is factually inaccurate or incomplete. If TU Dublin – City Campus holds and uses inaccurate personal data relating

to individuals, this can have a number of negative consequences for both individuals and TU Dublin – City Campus. Therefore, it is imperative that Functional Areas have in place appropriate procedures to enable them to deal with such requests promptly.

Where an individual requests their personal data to be rectified, Functional Areas are required to ensure the following:

- Respond without undue delay.
- Inform third party data processors of the rectification (where possible).
- Inform the individual about the third parties TU Dublin – City Campus have disclosed their data to (where appropriate).
- Where a Functional Area cannot action a request for rectification, it must explain why to the individual, and advise them of their right to complain to the Office of the Data Protection Commissioner (ODPC), and to right to seek a remedy through the courts.

5.3. Right to Access

A data subject has the right to access a copy of their personal data processed by TU Dublin – City Campus. In addition, the right to access personal data allows data subjects to be aware of and verify the reasons for which TU Dublin – City Campus is using their personal data.

Individuals have the right to obtain the following:

- Confirmation as to whether TU Dublin – City Campus process their data.
- A copy of their personal data.
- In addition they have the right to be informed of the following:
    - the purposes for which TU Dublin – City Campus use their data;
    - the types of personal data that TU Dublin – City Campus hold about them;
    - the third parties that processed personal data on TU Dublin – City Campus s behalf;
    - how long TU Dublin – City Campus keeps personal data it processes;
    - their rights in relation to their personal data, e.g. right to erasure, rectification, restriction, object, and data portability;
    - their right to complain to the Office of the Data Protection Commissioner;
    - if TU Dublin – City Campus has not obtained their personal data from them directly, the source from where it was obtained;
    - if TU Dublin – City Campus uses automated decision making in relation to the data subject or profile then TU Dublin – City Campus is required to explain the logic involved in these processes and what consequences this may have for them;
    - If TU Dublin – City Campus transfers their personal data internationally and if so what safeguards TU Dublin – City Campus has in place to protect their data.

Once a request to access (Data Subject Access Request – DP SAR) is received, TU Dublin – City Campus must reply to this request within one month (30 calendar days), with the possibility of extending this by up to two months where the request is complex or onerous. Due to the strict timelines imposed on TU Dublin – City Campus to comply with the right to access, it is imperative that TU Dublin – City Campus ensure the following:

- When a Functional Area receives a DP SAR, it has to notify the IGO and DPO immediately to confirm the receipt of the request and provide a copy of the information free of charge.

- The IGO and DPO in conjunction with the Functional Areas must confirm the receipt of the request and provide a copy of the information free of charge.
- The IGO and DPO will notify the relevant Functional Areas of the DP SAR to ensure that it is managed appropriately.
- Where a DP SAR is manifestly unfounded or excessive TU Dublin – City Campus can charge a reasonable fee based on administration costs.
- Information must be provided by the IGO and DPO in conjunction with the Functional Areas to the data subject without delay and at the latest within one month of receiving the request.
- The time for compliance can be extended by a further two months where requests are complex or onerous. However, if this is the case the IGO and DPO in conjunction with the Functional Areas must inform the data subject within one month of receiving the request and explain why the extension is necessary.
- The IGO and DPO in conjunction with the Functional Areas has to ensure to verify the identity of the person making the request using reasonable means.
- If the request is made electronically the IGO and DPO in conjunction with the Functional Areas should provide the information in a commonly used electronic format (e.g. PDF etc.).
- Where Functional Areas hold a large amount of personal data about an individual they can ask the individual to specify the information that they would like to access.
- As not all personal data can be disclosed, the IGO and DPO in conjunction Functional Areas have to ensure that the data is screened prior to release by all applicable functions, and that a record of the response is retained in the Information Governance Office.

The first relevant factor in considering a DP SAR will be to understand what is meant by personal data, i.e. the information must identify the individual (please refer to **Appendix 2** for the relevant definition). Secondly, the Functional Areas must conduct a search as to whether they hold any personal data relating to the individual who has made the DP SAR.

The personal data processed by TU Dublin – City Campus dictates the scope of the DP SAR. Therefore, the data subject may provide an ID number (e.g. student ID, patient ID, employee ID or name) as a reference to their relationship with the University. However, the scope of the DP SAR may be broader than just that particular ID number. For example, a data subject may provide their employee ID because they are employed by the University presently and student ID because they completed a TU Dublin – City Campus Programme in the past. They may also have been patients at the Student Medical Health Centre while being a student at TU Dublin – City Campus. Therefore, data subjects may have come in contact with TU Dublin – City Campus across a number of functions.

Information to be reviewed for the DP SAR includes, (but is not limited to), personal data from the following sources:

- Paper and electronic data, e.g. application forms, file notes, memos, reports, and records stored in filing cabinets or on business systems.
- Emails.
- Formal typed material and hand-written entries whether formal or informal.
- Screenshots and system notes, if they include additional personal data.
- CCTV – data subjects are entitled to photographs and CCTV images held by TU Dublin – City Campus if they specifically request same and give relevant dates and times to enable retrieval of the data. Personal data (e.g. images) of other individuals in the photographs or CCTV images must be redacted.
- No type/category of document can be excluded; the content/information must be considered for release.

- If the same personal data is on two or more systems or accessible via two or more systems data from one system should only be given out.
- Data held by third parties processors has to be reviewed when fulfilling a DP SAR. The third party should be contacted to review data held and consider its release. Procedures should be agreed and put in place at the outset with the third party processor when entering into any business arrangement/contract.
- It is important that relevant data retention and disposal periods are adhered to. However, if data is retained longer than the stated retention period, it must also be considered for release as part of the DP SAR.

5.4. Right to Erasure

The right to erasure, which is often referred to as ***'the right to be forgotten'***, is a data subject's right to request to have their personal data deleted where there is no compelling reason for TU Dublin – City Campus to have it. It should be noted that this is **not an absolute right**. Functional Areas will only have to comply with the right to erasure if one of the following circumstances applies:

- The personal data is no longer necessary in relation to the purpose for which the Functional Area first collected it.
- The data subject withdraws consent.
- The data subject objects to the processing and there is no overriding legitimate reason to continue holding or using the personal data.
- The processing of the personal data is in breach of the GDPR.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to offering an online service to a child. The GDPR places extra requirements on TU Dublin – City Campus where it is collecting and using children's data therefore where Functional Areas are processing children's data they must pay special attention to existing situations where a child has given consent to processing and later requests erasure of the data.

In addition to the request having to satisfy one of the criteria above, there are also specific circumstances where the right to erasure does not apply and Functional Areas can refuse to deal with a request. Functional Areas can refuse to comply with a request for erasure where they process the data for one of the following reasons:

- Comply with a legal obligation.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- Exercise or defend legal claims.

5.5. Right to Restrict Processing

The right to restrict processing is a data subject's right to stop the processing of their personal data. Where this is the case, TU Dublin – City Campus is permitted to store the personal data, but not to use it further**.** In other words, Functional Areas can retain just enough information about the individual to ensure that their right to restriction is respected in the future.

Functional Areas are required to restrict the processing of personal data in the following circumstances:

- Where an individual believes that the personal data is inaccurate, Functional Areas have to restrict the processing until they have verified the accuracy of the data.

- Where the individual objected to the processing, and Functional Areas are considering whether their legitimate reason for processing the data overrides those of the individual.
- Where Functional Areas no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

5.6. Right to Object

Data subjects have the right to object to processing of their personal data in the following cases:

- The processing of their personal data is based ('lawful basis') on TU Dublin – City Campus's legitimate interests.
- Direct marketing (including profiling).
- Processing for purposes of scientific/historical research and statistics.

Function Areas must stop processing the personal data when a request to object to that processing is received, unless:

- Functional Areas can demonstrate compelling legitimate grounds for the processing (i.e. that there is a legitimate reason for continuing to use their data which overrides the interests of the individual).
- The processing is necessary for establishing, exercising or defending any legal claims.

If Functional Areas receive requests to object to the processing for direct marketing purposes, they must stop processing personal data for this purpose as soon as they receive an objection. There are no exemptions or grounds to refuse. Functional Areas must deal with an objection to processing for direct marketing at any time and free of charge. Refer to **Direct Marketing Policy** in **Chapter 8** for more requirements to processing personal data for direct marketing purposes.

If Functional Areas receive requests to object to the processing for research purposes, Functional Areas can request individuals to demonstrate sufficient grounds for exercising their right to object to processing for research purposes. Functional Areas can refuse to grant this right if processing is required to carry out a task for public interest.

In addition to the requirements outlined in this Policy, Functional Areas must explicitly inform individuals of their right to object when first collecting their personal data and this should be presented clearly and separately from any other information.

5.7. Automated Decision Making and Profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human interaction. In order to comply with the requirements outlined in this section Functional Areas are required to identify whether any of their processing activities amount to automated decision making and update their procedures accordingly.

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, e.g. rejection of an employment offer.

In order to comply with individuals' rights regarding automated decision making and profiling Functional Areas are required to ensure that there are mechanisms in place to provide individuals with the following options:

- Obtain human intervention during the decision making process;
- Express their point of view; and

- Obtain an explanation of the decisions made, and challenge them.

Functional Areas are **not** required to stop automated decision making in the following cases:

- Decision is necessary for entering into or performance of a contract between TU Dublin – City Campus and the individual.
- Decision is authorised by law (e.g. for the purposes of fraud or tax evasion prevention).
- Decision is based on explicit consent.

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on the data subject, e.g. rejection of employment.

Where Functional Areas process personal data for profiling purposes, they are required to ensure that appropriate safeguards are in place. Profiling is any form of automated processing intended to evaluate certain personal aspects of an individual, e.g. to analyse or to predict their performance at work or studies, etc. The safeguards includes the following:

- Ensure processing is fair and transparent by providing meaningful information to the data subjects about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate measures to enable inaccuracies to be corrected, and minimise the risk of errors.
- Keep personal data secure. Please refer to the TU Dublin – City Campus ***ICT Information Security Policies*** available on the TU Dublin website for detailed requirements for technical measures.

In addition, Functional Areas must ensure that automated decisions **do not** concern a child or involve the use of sensitive data. Sensitive data can be used in automated decision making only in the following circumstances:

- Data subjects have given an explicit consent; or
- The processing is required by law.

5.8. Right to Data Portability

A data subject has the right to access personal data which he/she provided to TU Dublin – City Campus in a structured, commonly used and machine readable format. Furthermore, the data subject has the right to transmit that data to another organisation. The right to data portability complements an individual's right to access their personal data (see **section 5.3**).

The following conditions must be in place for the right to data portability to apply:

- Where the lawful basis on which the personal data is processed is based on:
    - A data subject's consent (or explicit consent if special categories data); or
    - The performance of a contract to which the data subject is party.
- Where the processing is carried out by automated means (therefore the right to portability will not apply to paper files).
- Where personal data (including pseudonymous data, i.e. data that can be linked to the individual) is related to the data subject.
- Where the personal data has been provided either:
    - Knowingly by the data subject, e.g. name, address etc.; or
    - Observed data provided by the data subject through their activities, e.g. location data.

- Where other people's rights are not affected (e.g. third parties still must be able to assert their rights under the GDPR).

In order for Functional Areas to fulfil a request for data portability, they have to ensure the following:

- When a Functional Area receives a request for portability, it is required to provide a copy of the information free of charge.
- If an individual requests it, Functional Areas are required to transmit the data directly to another organisation if this is technically feasible.
- Information must be provided without delay, and at the latest within one month of receiving the request.
- The time for fulfilment can be extended by a further two months where requests are complex or onerous. However, if this is the case Functional Areas are required to inform the data subjects and explain why the extension is necessary.
- Functional Areas have to ensure to verify the identity of the person making the request using reasonable means.

5.9. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories, which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of ICT where required.

5.10. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Appendix 5.A. Subject Access Request Form

Request for a copy of Personal Data

3. Details of Requestor:

Surname: _____

Postal Address: _____

_____

Telephone / Email: _____

2. Details of Request:

I, _____, wish to have access to personal data that I believe TU Dublin – City Campus retains on me as outlined below: (**Please include student number or staff number if relevant**)

_____

_____

_____

_____

Signed: _____ **Date:** _____

Please return the completed form together with a copy of proof of identity by post to: Information Governance Officer and Data Protection Officer Technical University Dublin – City Campus, 5th Floor, Park House Grangegorman, 191 North Circular Road, Dublin 7, D07 EWV4 or by email to foi@dit.ie

1. For Office Use:

Data Received: _____ **Date of response to requestor:** _____

Appendix 5.B Data Subject Rights Request Management Procedure

Case Name	One Month Period (begin date-end date)	Managed by

Phase	Procedure	Completion Initials and Date
Define		
1.0	Subject Access Request received	
1.1	Nature of Request Request for additional copies of personal data	
1.3	Proof of Identification received	
1.4	Scope of request is clear	
1.5	Respond to request to either: advise of one month period advise of extension (up to three months in total) advise of fee (detailing the administrative costs of providing: information or communication or taking action related to an unfounded or excessive request – explain why you believe request to be unfounded or excessive additional copies of personal information refuse to act on the request: explaining why you believe request to be unfounded or excessive advise that no action will be taken: (and advise that the data subject may lodge a complaint with the supervisory authority and seek a judicial remedy request more information: concerning the request itself to confirm the identity of the data subject	
1.6	Record on Risk Register / DSAR log	
Data Collection		
2.0	Identify and Advise Stakeholders on request and timelines (Team members, IT, Legal Advisor)	
2.1	Identify sources of data (electronic files, emails, manual files, other)	
2.2	Identify search criteria (requestors name, variations on that name, address, any other personally identifiable data)	
2.3	Identify any employees involved in this particular case (these can be past or present)	
2.4	Search Criteria signed off by IT and Head of Function/School	
2.5	Provide search criteria to IT and Head of Function/School	
2.6	The location of the files on file shares to be identified, signed off, collected by IT. Any hard copies identified and scanned.	
Data Review		
3.0	All collated data to be given to IT for discovery and download to central location	
3.1	Access codes arranged for any reviewers to access central location	
3.2	Manager to meet team/reviewers to agree on review approach and necessary mechanics	
3.3	Head of Function/School and IGO and DPO to do first level review: Omit duplicates identify and omit data the requestor already has access to identify and redact data which mentions but is not 'about' the requestor redaction of any third party names and information	

	redaction of any information that does not relate to the requestor	
3.4	Senior Staff/Management to carry out second level review and redaction	
3.5	Executive Management to carry out Final review with outside counsel advice for complex issues or for overall assurance	
Delivery		
4.0	Complete discover, review compilation, and upload to secure self-service web interface	
4.1	Communicate username and password separately to data subject	
4.3	Update Subject Access Request Register and keep copy of all information provided to Requestor	

Chapter 6. Privacy by Design and Data Protection Impact Assessment Policy

Privacy by Design is an essential requirement that involves minimising privacy risks to individuals. It is the consideration of data protection implications at the start or re-design of any product, service, system, IT application or process that involves the processing or personal data. It fosters a culture of embedding privacy by design into operations and ensuring proactivity instead of reactivity.

Privacy by Default promotes that, where possible, having regard to business implications and the rights of the data subject, the strictest data protection settings are applied automatically to any project.

A Data Protection Impact Assessment (DPIA) is a tool, required by GDPR, which can help TU Dublin – City Campus to identify the most effective way to comply with its data protection obligations and meet individuals' expectation of privacy, and in turn, allow the identification and remediation of risks in the early stages of a project. Therefore, DPIAs are an integral part of taking a privacy by design approach to help ensure privacy by default.

6.1. Privacy by Design and by Default

Data Protection and Privacy legislation requires TU Dublin – City Campus to demonstrate that it is compliant with the data protection principles. In particular, TU Dublin – City Campus must implement appropriate measures to support compliance with these principles (please see **Appendix 2** for a list of the data protection principles) when developing and designing new products, services and applications. In order to do this, TU Dublin – City Campus must:

- Implement appropriate technical and organisational measures to meet the requirements of privacy by design and by default whilst taking into account the states of the art, the cost of implementation, the nature, the scope and purposes of the processing as well as the likelihood and severity of risks on individuals posed by the processing.
- Put in place necessary safeguards to protect the rights of individuals in relation to their personal data.
- Put in place measures ensuring that by default, only personal data which is necessary for each specific purpose of the processing are used. This applies to the amount of personal data collected, the extent of their processing, their storage period and their accessibility.
- Ensure that personal data cannot be accessed by an indefinite number of people without the data subject's intervention.

To support TU Dublin – City Campus in adopting a data protection by design approach to the way in which it processes personal data, Functional Areas are required to carry out the following:

- Identify areas where a DPIA would be required, and relevant, in the context of their processing activities and assess the risk posed to individuals by their processing activities.
- Implement appropriate measures to ensure compliance with the data protection principles when they are processing personal data (ensuring that they take into consideration the nature, scope and context of the processing they undertake).
- Carry out a DPIA ensuring the requirements set out in Appendix 6.A (criteria to determine whether a DPIA is required), Appendix 6.B (how to conduct a DPIA) and Appendix 6.C (DPIA template) are met and document decisions taken and actions arising out of the DPIA.
- Carry out a review to assess if processing is performed in accordance with the DPIA and if there is a change in the risk represented by the processing.
- In any event, carry out a review of the completed DPIA after 3 years.

6.2. Data Protection Impact Assessments

When a Functional Area undertakes a processing activity (e.g. a new IT system) which would be likely to have privacy impact upon students/patients/employees they should conduct a Data Protection Impact Assessment (DPIA) of these risks and identify measures, which would help to reduce these risks.

Although DPIAs are a useful tool for many kinds of projects that involve the processing of personal data, the GDPR requires TU Dublin – City Campus to carry out DPIAs where the processing would be likely to result in a high risk to individuals. **Such assessment is also recommended for high-risk data processing, which has taken place before May 2018 to ensure that the privacy risks to individuals are still mitigated.**

Appendix 6.A sets out the criteria to determine whether a DPIA is required, and **Appendix 6.B** demonstrates how to conduct a DPIA. **Appendix 6.C** provides a DPIA template.

6.2.1. When is a Data Protection Impact Assessment required?

Carrying out a DPIA is not mandatory for every type of processing activity that TU Dublin – City Campus undertakes. A DPIA is only mandatory where the processing of personal data is likely to result in a high risk to the rights of individuals, particularly where a new technology is being used. Refer to **Appendix 6.A** for criteria when DPIA should be carried out, and **Appendix 6.C** for a template for a DPIA.

Before Functional Areas embark on processing which may be considered as high risk, they must carry out an assessment of the impact on personal data of the envisaged processing operations. In order to determine whether the processing is likely to result in a high risk, the following factors should be considered:

- Evaluation or scoring, including profiling and predicting.
- Automated decision having a legal or similar significant effect.
- Systematic monitoring.
- Processing of special categories of personal data (sensitive data).
- Data processed on large scale.
- Datasets that have been matched or combined.
- Data concerning vulnerable data subjects.
- Innovative use of technology.
- Data transfer across borders outside the European Union (“EU”).
- When the processing itself prevents individuals from exercising a right, or using a service, or a contract.

The more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of the individuals (or data subjects), and therefore more likely it is that a DPIA is required.

In addition, a DPIA may be required if an existing processing activity changes and as a result presents a high risk to the rights of individuals. In cases where it is not clear whether a DPIA is required, it is still a useful tool to help TU Dublin – City Campus comply with GDPR.

6.2.2. When is a DPIA not required?

Functional Areas are **not** required to carry out a DPIA in the following cases:

- Where the processing is not likely to result in a high risk to the rights and freedoms of individuals.
- Where the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has already been carried out.

- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out.

6.2.3. When should the DPIA be carried out?

Functional Areas should start the DPIA as early as practical in the design of the project/system/service etc. even if some of the detail has not yet been decided. As the DPIA is updated throughout the lifecycle of a project, it will ensure that data protection and privacy are considered, and will promote the creation of solutions which enable compliance. The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. In some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.

6.2.4. What is the process for conducting and completing a DPIA?

Functional Areas must conduct, input and validate their own DPIAs, while liaising with the IGO and DPO throughout the process. The final review and approval of a Data Protection Impact Assessment from a Head of Function is a matter for the TU Dublin – City Campus GDPR Steering Group.

The Functional Areas should consult with other TU Dublin – City Campus stakeholders where necessary (e.g. ICT Service team). It may also be appropriate to seek advice from independent experts, i.e. external lawyers, security experts etc.

TU Dublin – City Campus should seek the views from individuals on the intended processing, where it is appropriate to do so. Functional Areas should document their justification for not seeking the views of data subjects if they decide that this is not appropriate.

If a Functional Area engages a data processor (a third party), the data processor may carry out/assist with the DPIA under the instruction of the Functional Area.

Functional Areas are required to maintain documentation of the DPIAs carried out and the risks, measures and decisions arising from the DPIA. Functional Areas must ensure to keep records of the DPIA process and provide them for review when requested by the IGO and DPO or other parties as part of compliance reviews or audits (e.g. audit by Data Protection Commissioner).

6.2.5. What should a DPIA contain?

The DPIA must address and contain the following information:

- A description and purposes of the processing of personal data, including TU Dublin – City Campus's legitimate interest in carrying out the processing.
- An assessment of the necessity and scale of the processing activity in relation to the purpose. The outcome of the assessment should be taken into account when determining the appropriate controls which should be implemented.
- An assessment of the risks to the data subjects, including the considerations of the following:
    - the likelihood and severity of the risk; and
    - the impact of the risk (e.g. identity fraud, financial loss etc.)
- The controls in places to address the risks, including the following:
    - Appropriate technical measures (e.g. relevant security measures etc.)
    - Organisational measures (e.g. robust policies, staff training etc.)

Where the output of a DPIA indicates that the processing involves a high risk which a Functional Area cannot mitigate, the Head of Function in TU Dublin – City Campus is required, with the input of the IGO and DPO, to consult with the Office of Data Protection Commissioner ("ODPC") where this is the case.

Refer to **Appendix 6.C** for a DPIA template.

6.3. On-going management of a DPIA

The DPIA must be a living document throughout the lifecycle of the processing and Functional Areas must ensure that it is kept up-to-date at all times. As a matter of good practice, at the very least, it should be re-assessed by the Head of Function after 3 years, and sooner if the nature of the processing changes in anyway as per above.

Risks can change as a result of change to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve quickly and new vulnerabilities can arise. Therefore it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over longer time.

Where necessary, the Head of Function will conduct a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations. This would be the case where a significant change to the processing operation has taken place in terms of context, risks, purposes, personal data processed, recipients, data combinations, security measures and/or international transfers. Examples would include where a new technology has come into use or because personal data is being used for different purpose. In cases like this, the processing in effect becomes a new data processing operation and could require a new or revised DPIA.

Each DPIA must be tabled for review and approval at the TU Dublin – City Campus GDPR Steering Group and subsequently noted at the TU Dublin – City Campus Operations and Resources Committee (ORC).

Where necessary, the IGO and DPO may also independently conduct a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations.

6.4. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

6.5. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO Officer in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

Appendix 6.A. Data Protection Impact Assessment – Criteria

The following criteria should be considered when determining whether a data protection impact assessment is required:

- The GDPR requires that the carrying out of a DPIA is mandatory where the processing of personal data is 'likely to result in a high risk to the rights and freedoms of natural persons'.
- A DPIA is required on any new data processing technology.

High Risk requiring a DPIA

Some examples of 'High Risk' processing are listed, but limited to:

The processing of personal data involves:

- **Evaluation or scoring**, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (GDPR recital 71 and 91).
- **Automated-decision making with legal or similar significant effect:** processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals.
- **Systematic monitoring:** processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c)). This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).
- **Sensitive data:** this includes special categories of data as defined in Article 9, (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data and financial data. In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by an individual in the course of purely personal or household activity (such as smart technology, cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.
- **Data processed on a large scale:** the GDPR does not define what constitutes large-scale, although recital 91 notes that 'large-scale processing operations aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.' The following factors, in particular, should be considered when determining whether the processing is carried out on a large scale:
    - the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
    - the volume of data and/or the range of different data items being processed;
    - the duration, or permanence, of the data processing activity; and

- the geographical extent of the processing activity.

- **Datasets that have been matched or combined**, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

- **Data concerning vulnerable data subject:** the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data.

- **Innovative use or applying technological or organisational solutions,** like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help TU Dublin to understand and to respond to such risks.

- **Data transfer across borders outside the European Union** taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.

  When the processing in itself **"prevents data subjects from exercising a right or using a service or a contract"** (recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

The more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. A processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA. In some cases, a processing meeting only one of these criteria will require a DPIA. Conversely, if a Functional Area believes that despite the fact that the processing meets at least two criteria, it is considered not likely to be high risk, the Functional Area must thoroughly document the reasons for not carrying out a DPIA.

Where appropriate, TU Dublin – City Campus will seek the views of data subjects or their representatives (e.g. Trade Union consultation prior to processing employee personal data) on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Appendix 6.B. How to conduct a DPIA

The DPIA Process

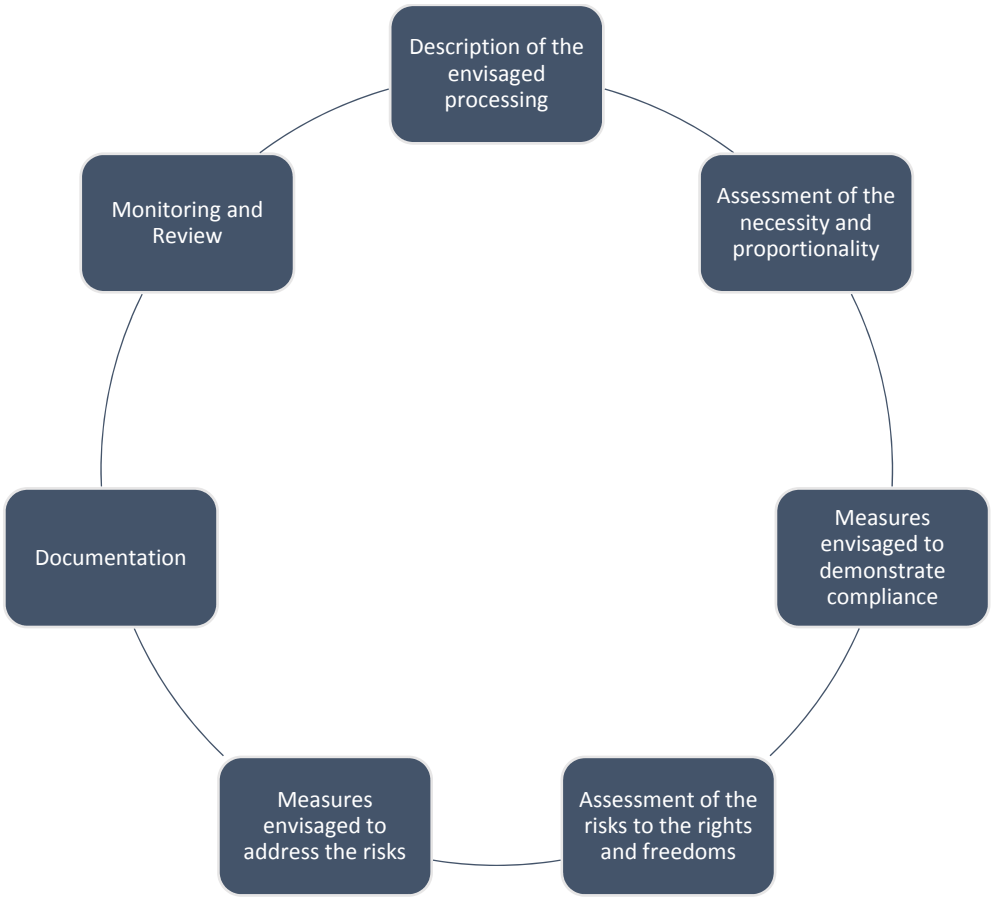


Diagram 1: The DPIA Process[1]

Description of the envisaged processing

Functional Areas are required to describe the information flow involved in the processing. This should include the following:

- nature, scope, context and purposes of the processing;
- personal data, recipients and period for which the personal data will be stored;
- a functional description of the processing; and
- the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels).

When codes of conduct (outlined in the GDPR) are put in place, the description of processing will have to include measures taken to comply with these codes of conduct.

[1] "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" issued by Article 29 Data Protection Working Party. Under the GDPR Article 29 Data Protection Working Party was replaced by the European Data Protection Board (EDPB).

Assessment of the necessity and proportionality

Functional Areas are required to assess whether the impact on privacy is necessary and proportionate to the outcomes of the project/system/service etc. Documentation of the measures outlined in the sections below will assist with this.

Measures envisaged to demonstrate compliance

Functional Areas are required to describe the measures in place to support compliance with the GDPR, taking into account the following:

- the measures contributing to the proportionality and the necessity of the processing on the basis of the following:
    - specified, explicit and legitimate purposes;
    - lawfulness of processing;
    - adequate, relevant and limited to what is necessary data; and
    - limited storage duration.
- the measures contributing to the rights of the data subjects, which includes the following:
    - information provided to the data subject;
    - right of access and data portability;
    - right to rectify, erase, object, restriction of processing;
    - recipients of individuals personal data (internally, externally);
    - data processors (third parties);
    - safeguards surrounding international transfer; and
    - prior consultation.

Assessment of risks

Functional Areas are required to document the risks involved in the processing. This should include the following:

- origin, nature, particularity and severity of the risks (e.g. unauthorised access, undesired modification, and disappearance of data), especially from the perspective of the data subjects;
- risks sources;
- potential impacts to the rights and freedoms of data subjects are identified in case of unauthorised access, undesired modification and disappearance of data;
- threats that could lead to unauthorised access, undesired modification and disappearance of data; and
- likelihood and severity of the identified risk.

Measures envisaged to address the risks

Functional Areas are required to identify what actions can be taken to reduce the risk to privacy for individuals. Depending on the nature of risks identified, measures could include the following:

- Deciding not to collect or store particular types of information.

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.

Following completion of the DPIA, where high risks remain, TU Dublin – City Campus will be required to consult the ODPC. The Head of Function in TU Dublin – City Campus is required with the input of the IGO and DPO to consult with the Office of Data Protection Commissioner ("ODPC") where this is the case.

Documentation

The various stages involved in the DPIA have to be documented. In particular, the identification of risks and measures that pose treat those risks. In addition, any decisions/advice in relation to the DPIA should be documented, e.g. feedback and/or advice of the IGO and DPO. The DPIA outcomes should be recorded and fed back into the project. Documentation is a key part of the DPIA process as it forms part of TU Dublin – City Campus's accountability for the data protection. In addition, the ODPC can request to inspect a DPIA, and it is TU Dublin – City Campus's obligation as a data controller to provide any relevant documentation to demonstrate compliance with the GDPR.

Appendix 6.C. Data Protection Impact Assessment Template

Any new product, process, system, contract, and / or use of end user or employee personal data need to be assessed for its privacy impact. Please address the following questions as comprehensively as possible.

PART I – INITIAL ASSESSMENT

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
1	**Name of Functional Area**	
2	**Project name** *(e.g. name of product, third party contract or new data project)*	
3	**Brief description of the project (new product or vendor services)**	
5	**Is any EU-based entity involved in the project?**	[Yes/No]
6	**Will the Functional Area collect, track, monitor or have access to any Personal Data (including Sensitive Personal Data) of end users through the product or vendor's service?**	[Yes/No} Note that Personal Data includes sensitive items such as: name, email address, date of birth, gender as well as IP address, device IDs and other unique identifiers Sensitive personal data includes: information relating to racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, genetic, health and sex life.
7	**If a vendor relationship, will any Personal Data of our end users be provided to, tracked, monitored or accessed by the vendor?**	[Yes/No]
8	**Does the project affect or touch EU-based end users? If so, please indicate countries.**	
9	**Will any Functional Area employee data be shared with the vendor under this agreement?**	[Yes/No]
10	**Will any other data (e.g., strategic, financial, proprietary or other sensitive DIT information) be shared with the vendor under this agreement? If yes, please provide details.**	[Yes/No]
Decision	**Is a formal DPIA required?**	[Please describe the decision in detail here]
Functional Area Data Protection Lead Signature		

[Part II on following page]

PART II –FULL ASSESSMENT

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
	Team members	
Section 1:	**Nature of the data**	
1.	**Please provide a list of all categories of data collected, used and disclosed. Please note that the definition of personal data is very broad (it incorporates all data and similar data set out in the examples below). This can either be data which has been explicitly provided by the individual to the Functional Area, or can also be data which is collected by Functional Area from other sources (internal schools or third parties), or even data which is collected by TU Dublin – City Campus automatically via cookies or other device identifiers.** **Please also provide details of whether this constitutes a change to the amount or types of data collected by the Functional Area, in comparison to the types of data it has collected up to now.**	
2.	**Please provide a list of "sensitive personal data," if any, involved?**	Sensitive personal data includes: information relating to racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, genetic, health and sex life. Please also include details of where the project involves the processing of criminal convictions or other criminal offences. If any of these categories of data are collected as part of the project, these should be listed here
3.	**If the project involves data accessed from, or stored in, an individual's device, please provide details.** *(For example, retrieving a MAC address from an individual's mobile phone or storing cookies on an individual's computer.)*	If, to collect data for the project, Functional Areas scan and collect information which is emitted from a device (such as a MAC address, which a device uses to assist with connecting to local Wi-Fi networks), please provide details of this here. Furthermore, if Functional Areas will store information on a user's device (for example a cookie being stored on a user's computer to ensure that their login details are remembered) then please provide details of each individual cookie or other identifier here.
Section 3:	**Responsibility for data uses**	

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
4.	**Who is the "owner" of the data used in the context of this project?** *(e.g. Business intelligence, analytics, marketing team, or Project team; please list all individuals)*	Please explain your response and provide details of the relevant Functional Areas (with help from Legal): Please describe the Functional Area which is responsible for collecting that data, will be responsible for ensuring its accuracy, and would have the right to sell or license that data on (if it were permitted by applicable laws). Please also set out which entities will have access to and will also be able to make choices about what the data will be used for.
5.	**Who is responsible for making decisions about the collection, use, storage and / or disclosure of data in the context of this project?** *(e.g. Business intelligence, analytics, marketing team, or Project team; please list all individuals)*	Please set out the Functional Areas, which collects the categories of data and makes choices about what the data will be used for.
Section 4:	**Compliance standards**	
	Transparency	
6.	**Are you aware of any steps taken to notify a data protection authority about the data processing activities relevant to this project?**	Please set out if the proposed project has been notified to or discussed with any data protection authority.
7.	**Will a data protection statement or privacy policy be used for the purpose of informing individuals of the uses and disclosures made of their data?**	Please explain whether the existing privacy policy covers the proposed uses of personal data, or if a separate notice will be provided to individuals. Please provide a link or an attached copy in each case.
	Legitimacy	
8.	**Will the Functional Area seek consent from individuals to use their data in the context of this project?**	If YES, please describe which uses for individuals' data Functional Area obtains consent in relation to. Please also explain when consent will be obtained from individuals, how it will be obtained (for example if it is obtained by users ticking a box on a website when they sign up for an account), and where it will be recorded.

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
9.	**Will any third party that discloses data to Functional Area in the context of this project obtain consent from individuals in respect of the use of the data by Functional Area?**	If YES, please describe which data obtained from third parties will be used on the basis of consent given to third parties. Please also explain how Functional Areas will ensure that appropriate consent has been given by third parties. For example, a Functional Area could obtain contractual protection from third parties, and could carry out due diligence on third parties by asking appropriate questions to ensure that appropriate consent has been obtained.
10.	**If the answer to the above questions regarding consent is NO, do any of the following cases apply:**	The data is necessary to provide a PROJECT/service. The data is necessary to comply with a legal obligation. The data is necessary to protect individuals. The data is necessary in the public interest. The data is necessary for Functional Area's interests and its use does not adversely affect individuals. Please provide further details about any options selected:
	Purpose limitation	
11.	**Please describe all of the intended purposes for which data is collected, used, stored and disclosed in the context of this project.** *(For example, for analytics purposes, for human resource management or vendor management purposes, to manage users, etc.)*	Please describe the purposes is a reasonable level of detail. For example, rather than simply 'analytics' or 'marketing', please use descriptions such as 'sending email marketing messages' or carrying out analytics on employee performance metrics. Other examples might be: human resource management purposes, managing employee contracts or vendor management purposes, to manage users, etc.
12.	**Is the data shared with any other party?** *(E.g. Facebook, Dropbox etc.)*	Please list the categories of entities that the Functional Area might share data with. For example, this might include service providers (where possible, list the types of services they might be providing such as human resources services or cloud storage services). In relation to each of these categories of recipients, please describe what purposes the third parties may use the data for and whether they will have the rights to make choices about the purposes for which the data will be used. For example, if data will be provided to third party service providers will those providers be restricted to acting on Functional Area‘s

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
		instructions, or will they be able to use the data for other products and projects.
	Proportionality	
13.	**Is <u>all of the data</u> collected or used necessary for the purposes identified above?**	For example, where CCTV cameras are installed on office premises, not all of that data will be used in the event that no criminal activity takes place or there is no reason to review it. The data is still collected on the basis that this is not known. In such a case, this description should be set out here.
	Quality	
14.	**How will data collected in relation to this project be maintained, kept accurate and up to date?**	Please explain how data will be stored. For example, will it be kept on an internal or cloud system? Please describe any ways in which Functional Area will ensure that, at the point of collection, the data collected is accurate. For example, when a user creates an account, will they be required to verify their email address (where an email is sent including a unique link to verify the address is real)? Please explain what functionality there will be to keep data up to date. For example, will it be possible for employees to update data fields, which inform them that they are incorrect?
15.	**How long will the data are retained for?** Please provide details of any periodic description / destruction of obsolete data if relevant.	Please explain how long data will be retained by the Functional Area. For example, this could state that employee data will be retained for as long as the individual is an employee, plus an additional two years, unless there is a reason to keep it longer. Please also explain how decisions on when to retain data beyond a usual period will be made: which functional area is able to make these decisions?
16.	**How will data be disposed of when is no longer required?**	

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
	Individuals' rights	
17.	**How will any requests from individuals be handled?** For example, complaints, enquiries, requests to opt-out, not to receive marketing communications or for access to information about the data held about them?	Please describe whether there are procedures which Functional Area has in place to handle requests to, for example, opt-out of marketing messages, have their data updated or deleted, access their data, object to profiling or other processing and restrict processing.
	Data security	
18.	**What security measures will be in place to ensure the confidentiality of data?**	Please describe the measures in place, for example what authentication procedures are in place (e.g. SSO, IP whitelisting). Are there organizational measures in place, such as restricted access based on an individual's role? Please also explain who determines the access level for each individual.
19.	**Will the use, collection, storage and disclosure of information in the context of this project be subject to any of the following:**	Please describe any of the following which apply: o Physical security measures (e.g. card access to rooms or buildings where data can be accessed) o An information security policy o Controls on access to information (e.g. password protection on all information, encrypted laptops and USB drives to access personal data only) o A business continuity plan (in the event of data loss) o Internal training programme on security systems and procedures (e.g. data protection training. Please also describe which relevant members of staff received such training) o Procedure to investigate breaches of security when they occur (please provide details of the principal steps in such procedure) o A recognised standard on information security standard (e.g. ISO/IEC 27002) Please provide further details about any options selected:

	QUESTIONS	PLEASE COMPLETE THIS COLUMN
20.	**Will any third party vendors process data on behalf of the Functional Area or collect data that will subsequently be used by Functional Area?**	Please describe each vendor and the service they provide to the Functional Area. For example, [vendor name]: payroll software. Please also attach copies of any written contract governing that relationship.
	International data flows	
21.	**Will the Functional Area share data with organizations based outside of Europe?** In providing your response, please also consider the locations of: ● Any servers on which Functional Area or vendors will process data. ● Any offices from which employees and vendor staff may remotely access servers processing data.	If YES, please provide details of each organisation the data will be shared with an indicate: o whether it is part of the TU Dublin – City Campus; o its geographic location; and o If there is a written contract governing the relationship?
Decision	**Does the processing result in a high risk to the rights and freedoms of individuals and require consultation with the Supervisory Authority?**	[Please document detailed decision]
Prepared by:		
Reviewed by the Information Governance Officer and Data Protection Officer:		
Signed off by the Head of Function:		
Reviewed by the TU Dublin – City Campus **GDPR Steering Group:**		

Chapter 7. Records of Processing Policy

Functional Areas that collect, use, transfer or store personal data of TU Dublin – City Campus's data subjects are required to document, manage and maintain records of processing within their function.

In line with GDPR records of processing need to be documented as a Personal Data Inventory (see **Appendix 7.A** for a template in a tabular form). This inventory reflects a Personal Data Lifecycle that graphically demonstrates the personal data flow from the point of collection of personal data by a Functional Area up to the point of its destruction (see **Appendix 7.B** for an example of personal data flow).

Refer to **Appendix 7.C** for a list of documented personal data flows and inventories currently in place within TU Dublin – City Campus.

7.1. Content of Records of Processing Activities

The record of processing at minimum has to contain the following:

- TU Dublin – City Campus's name and contact details.
- Name and contact details of the joint controller, where this applies (e.g., where a Functional Area enters a data sharing initiative with another organisation).
- Contact details of the IGO and DPO.
- The purposes of the data processing.
- A description of the categories of data subjects from whom the personal data is collected (i.e. patients, students, employees, children, etc.).
- Categories of personal data being collected and processed (e.g. personal data relating to medical history, student academic performance, payroll etc.).
- The types of third party organisations to which TU Dublin – City Campus might disclose personal data, including where TU Dublin – City Campus transfer data internationally.
- Description of safeguards that are in place where TU Dublin – City Campus transfers personal data internationally.
- If possible, the retention period for the different categories of personal data.
- If possible, a general description of the appropriate security measures in place to protect the data.

Head of Functions are responsible for keeping the records of processing and updating these records for any changes to the processing activities within their areas, e.g. changes in the retention period for personal data or implementation of a new business system used to process personal data.

In addition, TU Dublin – City Campus is required to provide the records of processing activities to the Office of the Data Protection Commissioner upon their request.

7.2. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

7.3. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Appendix 7.A. Personal Data Inventory Template

Data Controller details	
Name:	Dublin Institute of Technology. Academic Affairs
Telephone Number:	Please complete
Address:	Please complete
Email:	Please complete

Joint Data Controller details	
Name:	Please complete if applicable
Telephone Number:	Please complete if applicable
Address:	Please complete if applicable
Email:	Please complete if applicable

Data Protection Officer Details	
Name:	Please complete if applicable
Telephone Number:	Please complete if
Address:	Please complete if
Email:	Please complete if

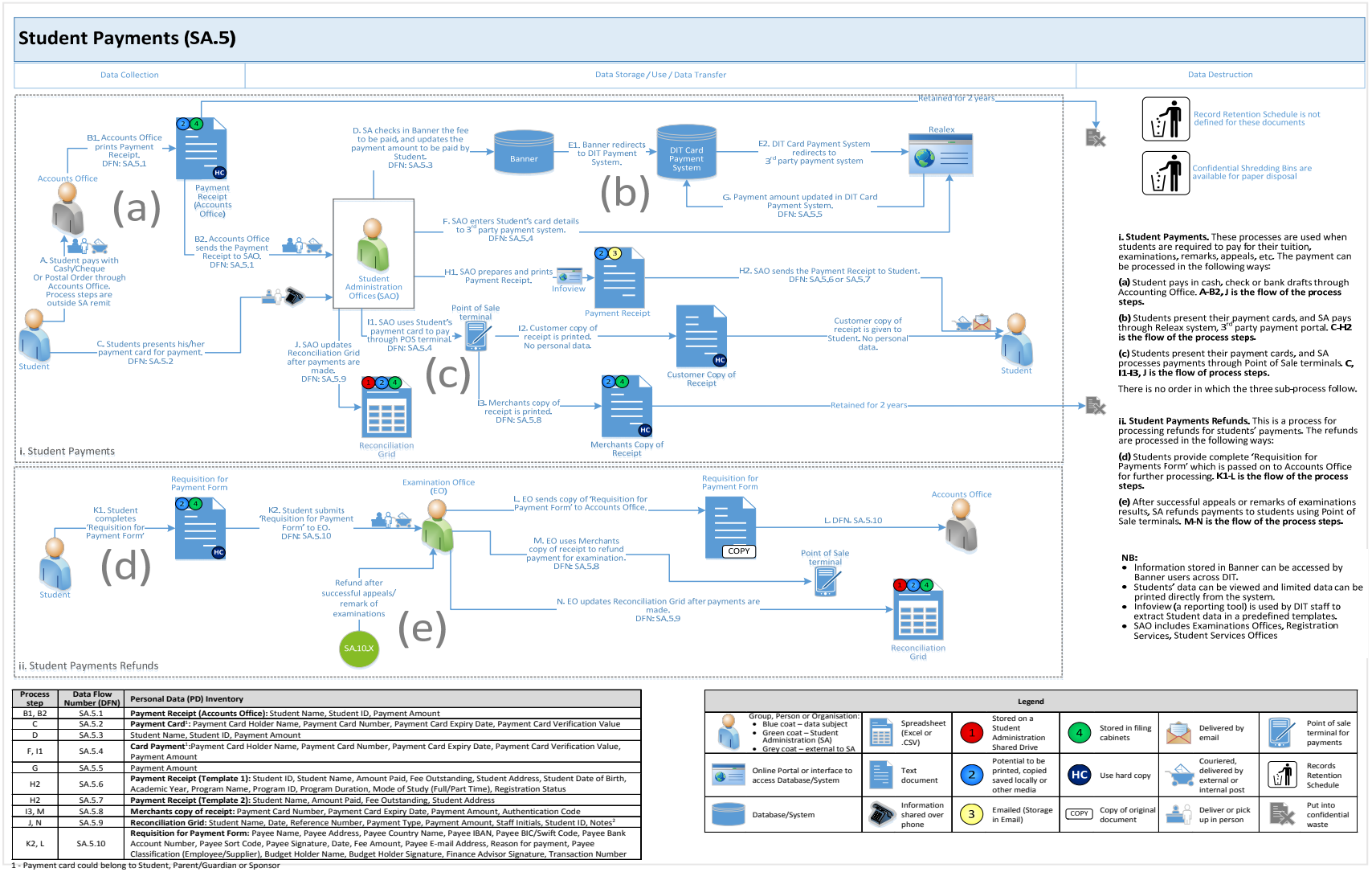
Document details	
Version:	1
Last Updated:	Apr-18
Next Reiew due:	Jun-18
Updated by:	Please complete

DEFINITIONS		CONTENT AND PURPOSE										
Data Subject	Data File/System	Identifiable fields	Data File/System Brief Description	Sensitive Data Processed	Criminal data and/or Children's data Processed	Process Name	Data Collected From	Data Collection Method	Purpose for Processing	Legal basis for processing	Internal Data Owner	Third Party Data Processor

FORMAT AND STORAGE							DATA DISCLOSURE						
Email Storage	Shared Drive Storage	Application Storage	Filing Cabinet Storage	Local Desktop Storage	Cloud Storage	Mobile Phone Storage	Data Disclosure (Internal, Intra-Group, External)	Categories of Data Recipients	Data Transfer outside EEA	Bases for transfer (consent, contracts, etc.)	Safeguards in place (Agreement / Contract / Bunding Corporate Rules)	Description of the safeguards in place	Security safeguards for data transfer

RETENTION				SECURTIY MEASURES			DATA LIFECYCLE REFERENCE
Data Retention	Relevant law and period of retention required	Policy or other documentation describing retention	Data Disposal (technique)	Geographic location where data is stored / Internal or External	Who has access to data	Access restrictions in place	Data Flow Ref. No.

Appendix 7.B. Example of a Personal Data Lifecycle



Process step	Data Flow Number (DFN)	Personal Data (PD) Inventory
B1, B2	SA.5.1	**Payment Receipt (Accounts Office):** Student Name, Student ID, Payment Amount
C	SA.5.2	**Payment Card**[1]**:** Payment Card Holder Name, Payment Card Number, Payment Card Expiry Date, Payment Card Verification Value
D	SA.5.3	Student Name, Student ID, Payment Amount
F, I1	SA.5.4	**Card Payment**[1]**:**Payment Card Holder Name, Payment Card Number, Payment Card Expiry Date, Payment Card Verification Value, Payment Amount
G	SA.5.5	Payment Amount
H2	SA.5.6	**Payment Receipt (Template 1):** Student ID, Student Name, Amount Paid, Fee Outstanding, Student Address, Student Date of Birth, Academic Year, Program Name, Program ID, Program Duration, Mode of Study (Full/Part Time), Registration Status
H2	SA.5.7	**Payment Receipt (Template 2):** Student Name, Amount Paid, Fee Outstanding, Student Address
I3, M	SA.5.8	**Merchants copy of receipt:** Payment Card Number, Payment Card Expiry Date, Payment Amount, Authentication Code
J, N	SA.5.9	**Reconciliation Grid:** Student Name, Date, Reference Number, Payment Type, Payment Amount, Staff Initials, Student ID, Notes[2]
K2, L	SA.5.10	**Requisition for Payment Form:** Payee Name, Payee Address, Payee Country Name, Payee IBAN, Payee BIC/Swift Code, Payee Bank Account Number, Payee Sort Code, Payee Signature, Date, Fee Amount, Payee E-mail Address, Reason for payment, Payee Classification (Employee/Supplier), Budget Holder Name, Budget Holder Signature, Finance Advisor Signature, Transaction Number

1 - Payment card could belong to Student, Parent/Guardian or Sponsor
2 - This is a free text field and can contain personal and sensitive data related to a Student

Appendix 7.C. Data inventories currently in place as of May 2018.

Functional Area	Personal Data-Lifecycle	Personal Data Inventory	Data Owner
Student Administration	1. Registration 2. Part-time Admissions 3. Deferral & Withdrawal 4. Fees 5. Student Payments 6. Student Cards 7. Invigilators 8. Examiner and Invigilator Payments 9. Exams 10. Exam Appeals 11. Exam Incidents 12. Apprentice Exams 13. Transcripts 14. Third Party Printing 15. Program Repeats 16. Sharing Student Data	Student Administration Inventory v1	Student Administration Office
DIT Foundation	1. Alumni Data Collection 2. Alumni Events 3. Communication Newsweaver 4. Non-Alumni relationship Management 5. Appeals 6. Donations 7. Sponsoring Students 8. Travel Sponsorships 9. Tax Returns	DIT Foundation Inventory v1	DIT Foundation
Academic Affairs	1. External Examiners 2. Assessor Appointments 3. Student Appeals 4. Disciplinary Records	Academic Affairs Inventory v1	Academic Affairs Office
Health and Safety	1. Risk Assessments 2. Allergy Questionnaire 3. Incident Report	Health and Safety Inventory v1	Health and Safety Office

Functional Area	Personal Data-Lifecycle	Personal Data Inventory	Data Owner
National Optometry Centre	1. Booking Patients for Appointments 2. Examinations 3. Post Examination 4. Treatment Benefit Schemes 5. Clinical Data Used for Teaching/Research		
Research, Enterprise and Innovation			
Fees and Income Office			
Library Services			
Payroll			
Human Resources			

Chapter 8. Direct Marketing Policy

TU Dublin – City Campus is an academic community of students and staff, in a higher education institution that is practice-based and research-informed, currently based on a number of different campuses across the city centre. To fulfil its public role as a practice-based institution, TU Dublin – City Campus endeavours to ensure that all members of our staff and student the community receive information about the wide range of activities being organised by colleagues and students in different disciplines and different locations and, in particular, where it concerns exhibition of students' work, performances, or presentation of research. Information about student and staff successes and achievements is also shared through TU Dublin – City Campus student and staff email addresses, e-zines and websites.

If information relates to colleagues' roles, or to students' courses, it is acceptable to share it through email, ensuring that the recipients' email addresses are not visible. Other information that does not specifically relate to these areas should not be shared in this way. Any form of marketing to such audiences must follow the TU Dublin – City Campus Direct Marketing Policy. For example, it must offer a way for people to 'opt out', and this preference should be recorded to ensure that they do not receive future communications.

This chapter highlights the key requirements a Functional Area are required to adhere when carrying out direct marketing to data subjects or businesses. It explains Direct Marketing and Data Protection requirements for Functional Areas intending to conduct Direct Marketing communicating with potential students, patients, funders, potential donors and other individuals when promoting TU Dublin – City Campus. Functional Areas must comply with legislative requirements and manage any potential or actual risk related to such activity.

Functional Areas will not always need to process personal data to carry out a direct marketing exercise. However, they must still comply with electronic marketing rules. Where Functional Areas do use personal data to conduct direct marketing, they must ensure to comply with the GDPR in addition to electronic marketing rules. For further guidance on GDPR requirements please see Data Protection Policy in Chapter 2.

Direct marketing can be solicited or unsolicited. Solicited marketing is marketing which has been specifically requested by the individual and providing that GDPR is complied with (refer to TU Dublin – City Campus Data Protection Policy, TU Dublin – City Campus Data Subjects Rights for more details on the requirements), there is no restriction on this. Electronic marketing rules will apply where the marketing is unsolicited, i.e. the marketing has not been specifically requested.

Legislation Governing Direct Marketing

Relevant Legislation	Scope	Applicability
Electronic Privacy Regulations 2011 ("EP Regulation") *	Electronic marketing in Ireland	• Customers/individuals • Companies
General Data Protection Regulation	Requirements in relation to processing personal data (including for direct marketing purposes)	• Identifiable Customers/Individuals attributed to companies i.e. Directors, Sole Traders and Partners)

***Please note that the proposed implementation of the ePrivacy Regulation will trigger reform of current electronic marketing rules.**

8.1. Electronic Marketing

TU Dublin – City Campus can use an individual's electronic contact details, including email and mobile phone number for the purposes of direct marketing (via telephone, email, SMS) when:

- The individual has consented to direct marketing within the last 5 years; or

- TU Dublin – City Campus has obtained the electronic contact details in the course of service (or event) within the last 12 months and the direct marketing material relates to a 'similar product or service', provided the individual was given an opportunity to refuse such contact at the time the data was collected, also known under electronic marketing rules as a 'Soft Opt – in'.

Note that 'Similar Products or Services' are defined as a like for like, of the same kind, nature or amount or having a similar resemblance. Functional Areas engaged in direct marketing activity are expected to pay close attention to the limitations which this definition sets down.

When Functional Areas use electronic marketing they have to ensure the following:

- If a Functional Area wishes to capture data subjects consent for future marketing activities during a TU Dublin – City Campus or not TU Dublin – City Campus events, it would be recommended to use an Opt – in (i.e. obtain explicit consent).
- Give individuals the opportunity to object to direct marketing in an easy manner and without charge, by offering an Opt-out option.
- Do not include a marketing message within email signatures.
- Before electronic email marketing by email Functional Areas are required to screen the names and addresses against the email preference consent.

If a Functional Area contacts individuals over the phone for marketing purposes, both for calls and SMS marketing, the Functional Areas have to ensure the following requirements are met:

- Data subjects have consented to phone marketing, including phone calls and/or SMS.
- Phone numbers have to be kept up-to-date in order to avoid contacting a wrong individual with marketing communications.
- Provide an opt-out option for phone marketing.
- Keep records of consents and opt-outs for phone marketing.

Refer to **section 8.4** for more requirements for a valid consent.

8.2. Postal Marketing

Electronic marketing rules only cover direct marketing through electronic means (telephone, email, SMS). Therefore, if Functional Areas are carrying out postal marketing, electronic marketing rules will not apply. However before Functional Areas can use personal data for postal marketing, they must ensure that the marketing is compliant with the GDPR. Refer to TU Dublin – City Campus Data Protection Policy, TU Dublin – City Campus Data Subjects Rights for more details on the requirements.

For postal marketing to be considered direct marketing it has to be addressed to a named person and must be promoting a product or service. Unaddressed mail sent to a household or business is not covered by GDPR as no personal data is used. The GDPR does not include market surveys seeking data subjects' views, e.g. opinion on political matters or radio listenership preferences.

8.3. Valid consent

Functional Areas are required to ensure that where consent is required for direct marketing that it is valid by meeting the following requirements:

- Consent must be freely given, specific, informed and unambiguous.
- Consent must be a clear, affirmative action. It is important to ensure that it is a positive affirmation, e.g. positive opt-in. Pre-ticked boxes or silence does not constitute consent.

- Consent for direct marketing purposes must be distinguishable, clear, and is not “bundled” with other written agreements or declarations, i.e. consent required for direct marketing purposes must be separate from consent for other types of processing activities.
- Be clear and concise when collecting consent.
- Be specific when collecting consent from individuals so they know exactly what they are consenting to.
- Name any third party controllers who will rely on the consent.
- Make it easy for individuals to withdraw consent, and provide information on how to withdraw.
- Keep evidence of consent – who, when, how, and what individuals were told when they provided consent. TU Dublin – City Campus is required to be able to evidence that consent is in place for direct marketing purposes as part of accountability responsibilities.
- Keep consent under review, and refresh it if anything changes.

8.4. Right to Object

Data subjects have the right to object to direct marketing (including profiling). Where an individual exercises their right to object to direct marketing, TU Dublin – City Campus must stop processing the personal data for these purposes immediately. Functional Areas must deal with an objection for processing at any time and free of charge. Refer to TU Dublin – City Campus Data Subject Rights Policy for details.

8.5. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO (email foi@dit.ie) in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

8.6. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas may have to provide these records to IGO and DPO for inspection or consultation.

Chapter 9. Data Processor Management and Data Transfer Policy

The type of third party governance arrangements required will depend on the nature of TU Dublin – City Campus's relationship with a third party. That is, whether they are data controller or a data processor.

Therefore a key step in determining the appropriate governance arrangements is to identify the role of the third party in the data processing relationship.

To ascertain whether the third party is a data controller or processor, the following factors should be considered:

- Who decides to collect the personal data in the first place and the lawful basis for doing so;
- Which items of personal data to collect;
- The purpose/s the data are to be used for;
- Which individuals to collect data about;
- Whether to disclose the data, and if so who to;
- Whether subject access and other individuals' rights apply; and
- How long to retain the data or whether to make non-routine amendments to the data.

The above factors are all decisions which can only be taken by a data controller. A data controller will exercise overall control over the 'why' and 'how' of a data processing activity. A data processor may use its technical knowledge to decide how to carry out certain activities on the data controller's behalf. However it cannot take any of the over-arching decisions, for example what the personal data will be used for. Such decisions must only be taken by the TU Dublin – City Campus data controller.

The fact that an organisation provides a service to TU Dublin – City Campus does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises. For any questions regarding the role of the third party, the IGO and DPO should be consulted.

TU Dublin – City Campus can also act as a data processor to a third party. In these cases, TU Dublin – City Campus must act on instructions provided by a third party, which is a data controller. As a data processor, TU Dublin will provide necessary support to the data controller based on a data processing agreement and other contractual obligations. **Appendix 9.A** sets out a checklist in cases when TU Dublin – City Campus is a data processor.

9.1. Management of Data Processors

9.1.1. Selection of Data Processors

The GDPR outlines that TU Dublin – City Campus must only use data processors who can provide sufficient guarantees in terms of resources and expertise, to implement technical and organisational measures to comply with GDPR and protect the rights of individuals.

As part of the selection process, it is important to analyse the nature of the processing and level of risk posed to individuals to help ensure that the data processor can offer sufficient guarantees to protect their rights. Therefore, prior to the engagement of any third party processor Functional Areas have to carry out due diligence checks of potential third parties in relation to data protection compliance. The relevant data owner must inform the IGO and DPO of any new third parties being assessed so that they can input and offer advice in relation to this.

The following checks must be completed and evidence of completion must be retained by the Functional Areas:

- Ascertaining where the data is stored;

- Inspection of any relevant third party assurance reports on the control environment of the processor;
- Ascertaining if the processor has been inspected by the Data Protection Supervisory Authority and the results if applicable;
- Identifying if the processor has an appropriate privacy framework in place;
- Consider whether it is appropriate to require the use of specific technical measures, such as pseudonymisation or encryption;
- Consider requiring the processor to implement data protection by design where applicable;
- Identify if the processor has a IGO and DPO in place;
- Identify if the processor has the technical capability to facilitate data subject requests in relation to access, restriction, erasure and deletion in line with the retention schedule; and
- Identifying if the processor has adequate training and awareness programme in relation to data protection.

In addition to the above checklist, **Appendix 9.B** contains a checklist, which is useful to help data processors understand their obligations under the GDPR.

9.1.2. Contract Requirements

Following the suitability assessment, TU Dublin – City Campus is required to have in place a written contract with any data processor that it uses, which must contain certain specific terms laid out below. This is important as it helps both TU Dublin – City Campus and the data processor/s to understand TU Dublin – City Campus's responsibilities and liabilities. The checklist below should be used to ensure that each contract with processor contains the necessary requirements.

Contracts must include the following compulsory details:

- The subject matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subject; and
- TU Dublin – City Campus's obligations and rights.

Contracts must include the following compulsory terms:

- The processor acts on the written instructions of TU Dublin – City Campus (unless required by law to act without such instructions);
- The processor must ensure that people processing the data are subject to a duty of confidence;
- The processor must take appropriate measures to ensure the security of the processing;
- The processor must only engage a sub-processor with the prior written consent of TU Dublin – City Campus which should also be governed by a written contract;
- The processor must assist TU Dublin – City Campus in providing subject access and allowing data subjects to exercise their rights under GDPR;
- The processor must assist TU Dublin – City Campus in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- The processor must delete or return all personal data to TU Dublin – City Campus as requested at the end of the contract; and
- The processor must submit to audits and inspections provide TU Dublin – City Campus with whatever information it needs to ensure that they are both meeting their obligations GDPR and tell

TU Dublin – City Campus immediately if it is asked to do something infringing Data Protection and Privacy legislation.

As a matter of good practice TU Dublin – City Campus's contracts with data processors should:

- State that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under GDPR; and
- Reflect any indemnity that has been agreed.

9.1.3. Sub-contracted Data Processors

GDPR places further requirements on a data processor where they wish to employ another processor. It needs to obtain the written consent from TU Dublin – City Campus and put in place a written contract with the sub-contracted processor. The processor must inform TU Dublin – City Campus of any intended changes concerning the addition or replacement of other processors, thereby affording us the opportunity to object to such changes. Where the sub-contracted processor fails to fulfil its data protection obligations, the initial processor will remain fully liable to TU Dublin – City Campus for the performance of the sub-contract processors obligations.

9.1.4. Monitoring and Reporting

A log of all third party processors should be maintained by each functional area, which includes the following:

- Reference to the outcome of the due diligence exercise;
- Classes of data processed including sensitivity;
- Contract commencement date;
- Details in relation to any periodic audits, testing or monitoring;
- Contract expiry date.

The IGO and DPO will perform periodic monitoring of the log of third party processors to ascertain compliance with this policy. In addition, audits and inspections of processors will be carried out as detailed in the data processor contract in order for TU Dublin – City Campus to be able to demonstrate compliance with the accountability principle under GDPR.

Before sharing any personal data you hold, you will need to consider all the legal implications of doing so. Functional Areas' ability to share information is subject to a number of legal constraints. There may be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect Functional Areas' ability to share personal data.

Data sharing can take the form of:

- A reciprocal exchange of data;
- One or more organisations providing data to a third party or parties;
- Several organisations pooling information and making it available to each other;
- Several organisations pooling information and making it available to a third party or parties;
- Exceptional, one-off disclosures of data in unexpected or emergency situations; or
- Different parts of the same organisation making data available to each other.

If you wish to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, you need to consider whether you have the legal power or ability to do so. This is likely to depend, in part, on the nature of the information in question – for example, whether it is sensitive personal data.

9.2. Data Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third-party countries or international organisations, to ensure that the level of protection of individuals afforded by the GDPR is not undermined. The GDPR limits an organisation's ability to transfer personal data outside the EU where this is based only on that body's assessment of the adequacy of the protection afforded to the personal data. Ideally, transfers may be made where the European authorities have decided that a third country, a territory in that third country or an international organisation ensures adequate safeguards for the protection of data.

9.2.1. Appropriate Safeguard's

TU Dublin – City Campus may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. For further information of the data subjects rights, please see **Data Subjects Rights Policy in Chapter 5.**

Adequate safeguards may be provided for by:

- A legally binding agreement between public authorities or bodies;
- Binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- Standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- Standard data protection clauses in the form of template transfer clauses adopted by a Supervisory Authority and approved by the Commission;
- Compliance with an approved code of conduct approved by a Supervisory Authority;
- Certification under an approved certification mechanism as provided for in the GDPR;
- Contractual clauses agreed authorised by the competent Supervisory Authority; or
- Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent Supervisory Authority.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

9.2.2. Derogations for specific situations

The GDPR sets out the derogations or exceptions from the prohibition on transferring personal data outside the EU without adequate protections. The derogations apply when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.

- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register that, according to EU or member state law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

9.2.3. Once off transfer of personal data

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- Is not being made by a public authority in the exercise of its public powers;
- Is not repetitive (similar transfers are not made on a regular basis);
- Involves data related to only a limited number of individuals;
- Is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- Is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant Supervisory Authority of the transfer and provide additional information to individuals.

9.3. Data Sharing Agreements

Data sharing agreements – sometimes known as 'data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis. A data sharing agreement should, at least, document the following issues:

- The purpose, or purposes, of the sharing;
- The potential recipients or types of recipient and the circumstances in which they will have access;
- The data to be shared;
- Data quality – accuracy, relevance, usability etc;
- Data security;
- Retention of shared data;
- Individuals' rights – procedures for dealing with access requests, queries and complaints;
- Review of effectiveness/termination of the sharing agreement;
- Sanctions for failure to comply with the agreement or breaches by individual staff.

Data sharing arrangements review

Once a data sharing arrangement is in place, the appropriate manager should review it on a regular basis. This is because changes can occur and they need to be reflected in the data sharing arrangements to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

The following key questions should be considered regularly:

- Is the data still needed? There is the potential that the aim of the data sharing has been achieved and that no further sharing is necessary. On the other hand, there is the potential that the data sharing is making no impact upon its aim and therefore the sharing is no longer justified.
- Do the privacy notice and any data sharing agreements in place still explain the data sharing that is being carried out accurately?
- Are the information governance procedures still adequate and working in practice? All the organisations involved in the sharing should check:
    - Whether it is necessary to share personal data at all, or whether anonymised information could be used instead;
    - That only the minimum amount of data is being shared and that the minimum number of organisations, and their staff members, have access to it;
    - That the data shared is still of appropriate quality;
    - That retention periods are still being applied correctly by all the organisations involved in the sharing;
    - That all the organisations involved in the sharing have attained and are maintaining an appropriate level of security;
    - That staff are properly trained and are aware of their responsibilities in respect of any shared data they have access to.

9.4. Data transfer methods

Before choosing the method of transfer, the following items must be considered:

- The nature of the information, its sensitivity, confidentiality or possible value;
- The size of the data being transferred;
- The damage or distress that may be caused to the data subject(s) as a result of any loss during transfer; and
- The implications any loss would have for the University.

Functional Areas must only send information that is necessary for the stated purpose outlined in the privacy notice. Functional Areas must remove any unnecessary data, and any data not required should be redacted or removed completely (as appropriate) before transfer.

Refer to **Appendix 9.B** for data sharing checklist.

9.4.1. Email

All data sent over email (as an attachment or in an email text) should be considered sensitive and therefore should be protected. Never send work documents or information to someone outside of TU Dublin – City Campus unless it has been cleared by an information owner and TU Dublin – City Campus ICT. **This includes forwarding emails to TU Dublin – City Campus employees' personal email account.** As not all users within TU Dublin – City Campus have authorised access to the same

information, before sending data or files to a co-worker in an email, it should be checked that the recipient is required to have access to it.

9.4.2. Cloud storage and cloud applications

In some cases staff may need access to work outside of the office from home and on mobile devices. However, information relating to data subjects should never be stored or shared to personal cloud accounts or applications, such as iCloud, Google Drive, WhatsApp, Dropbox, Microsoft OneDrive, etc.

Should the data need to be stored or backed up online, this should only be done using an ICT-approved service.

9.4.3. Telephone / mobile phone

As phone calls may be overheard or intercepted either deliberately or accidentally, care must be taken as follows:

- Controlled data must not be transferred / discussed over the telephone unless you have confirmed the identity and authorisation of the recipient;
- When using answer phones do not leave sensitive or confidential messages, or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing.

9.4.4. Sending the information by post

As a part of its obligations TU Dublin – City Campus will routinely send letters containing personal information to TU Dublin – City Campus students, staff, patients etc. However, whilst this is routine, care must still be taken to ensure that the information is correctly addressed to a named recipient and information is not sent in error to the wrong recipient. Mail going to the wrong data subject is a danger to the individual whose information is being sent. It also puts TU Dublin – City Campus at risk of breaching its responsibilities under the GDPR. As a sender, TU Dublin – City Campus staff is responsible for making sure that:

- The postal address is correct;
- The envelope is clearly marked for the attention of the intended recipient;
- No information relating to another individual has been included in error, either in a letter/email or an attached document;
- That you choose the most appropriate method of transfer.

9.4.5. Hand delivery / collection

Hand delivery or collection of a document is also an approved method of transfer. However, if you are taking paper records off site you still need to ensure you are complying with this policy and the Data Protection Policy.

Also when arranging for an individual to collect information, you should satisfy yourself that they are who they say they are and seek an appropriate form of identification before you hand over any documentation.

9.5. Data Breach Notification

Although TU Dublin – City Campus retains overall responsibility for the protection of personal data, the processor has an important role to play to enable us to comply with its obligations; this includes breach notification. Therefore if the processor becomes aware of a breach of the personal data it is processing on TU Dublin – City Campus's behalf, it must notify TU Dublin – City Campus without undue delay. This will assist TU Dublin – City Campus in addressing the breach and to allow it to fulfil its obligations in terms of notifying breaches to the Data Protection Supervisory Authority and the affected individuals where relevant.

9.6. Monitoring and Compliance

The University is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The University as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by TU Dublin – City Campus (in both paper and electronic forms).

Any member of staff or student of the University, or other individuals who come into contact with TU Dublin – City Campus, and who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the IGO and DPO in the first instance.

The University as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by Functional Area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the IGO and DPO with the input and support of IS where required.

9.7. Accountability and Record Keeping

Head of Function is responsible for the implementation of the policy within their Functional Area, and develop and implement procedures to support the compliance with the policy. It is important that Functional areas keep records and audit trails of their data protection practices in order to demonstrate compliance with the policy.

Functional areas have to provide these records to IGO and DPO for inspection or consultation.

Appendix 9.A. TU Dublin Obligations as a Data Processor

A data processor has the following responsibilities under the GDPR:

- ☐ Only act on the written instructions of the controller
- ☐ Not use a sub-processor without the prior written authorisation of the controller
- ☐ Co-operate with Data Protection Supervisory Authorities
- ☐ Ensure the security of its processing activities
- ☐ Keep records of its processing activities
- ☐ Notify any personal data breaches to the controller
- ☐ Appoint (in writing) a representative within the European Union if required

A processor should also be aware that:

- ☐ It may be subject to investigative and corrective powers of Data Protection Supervisory Authorities
- ☐ If it fails to meet its obligations, it may be subject to fines
- ☐ If it fails to meet its obligations it may have to pay compensation to individuals

Appendix 9.B. Data Sharing Checklist

Is the sharing justified? Key points to consider:

- What is the sharing supposed to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share? Key points to consider:

- Any relevant functions or powers of your organisation;
- The nature of the information you have been asked to share (for example was it given in confidence?);
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share the data, it is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared?
    - Only share what is necessary;
    - Distinguish fact from opinion.
- The organisations that will be involved;
- What you need to tell the data subject(s) about the data sharing and how you will communicate that information;
- Measures to ensure adequate security is in place to protect the data;
- What arrangements need to be in place to provide data subject(s) with access to their personal data if they request it?
- Agreed common retention periods for the data;
- Processes to ensure secure deletion takes place.

Record your decision

Record your data sharing decision and your reasoning, whether or not you shared the information. If you share information you should record:

- What information was shared and for what purpose;
- Who it was shared with;
- When it was shared;
- Your justification for sharing;
- Whether the information was shared with or without consent.

Appendix 9.C. Data Processor Due Diligence Template

Note: the following checklist is strictly confined to data protection checks in relation to a third party processor.

Due Diligence Checklist

The following checks must be completed and evidence of completion must be retained by a contract owner and/or Head of Procurement.

- ☐ Establish that there is a written contract or agreement in place which includes standard form data protection clauses;
- ☐ Ascertain whether or how often the vendor / third party contractor has experienced cyber security / data protection incidents;
- ☐ Ascertain the category and types of data that may be transferred processed by the vendor / third party contractor;
- ☐ Ascertain where the data is stored; (*particularly important where data is stored outside Europe. Also of importance given the UK's decision to exit the EU);
- ☐ Inspection of any relevant third party assurance reports on the control environment of the processor;
- ☐ Ascertain if the data processor has been inspected by the *relevant supervisory authority* and the results if applicable;
- ☐ Verify if data processor has an appropriate privacy framework in place;
- ☐ Consider whether it is appropriate to require the use of specific technical measures, such as pseudonymisation or encryption;
- ☐ Consider requiring the data processor to implement data protection by design where applicable;
- ☐ Identify if the data processor has a IGO and DPO in place, where relevant;
- ☐ Identify if the data processor has the technical capability to facilitate data subject requests in relation to access, restriction, erasure and deletion in line with the retention schedule; and
- ☐ Identify if the data processor has adequate training and awareness programme in relation to data protection.

Approved by: **Date:**

[Role]

Reviewed by: **Date:**

Information Governance Officer and Data Protection Officer

Appendix 1. Data Protection Principles

The data protection principles as outlined in the GDPR are a set of requirements, which the Functional Areas have to follow when processing personal data. The principles require that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner.

The GDPR requires the need for transparency over how the Functional Areas use personal data. For Functional Areas this means:

- They should make it clear to individuals how their information is collected, used, consulted or otherwise processed, and to what extent their information will be processed in the future. This must be conveyed in an easily accessible and easy to understand way in clear and plain language.
- They must make individuals aware of who is processing their data and the explicit and legitimate purposes for which it is used (which should be determined at the time their data was first collected).
- They must make individuals aware of the risks, rules, safeguards and rights in relation to the processing of their information.
- In order to lawfully process personal data (and special categories data) they must be able to identify relevant lawful bases, e.g. consent, necessary for the performance of contract etc.
- Where consent has been identified as the lawful basis, Functional Areas must ensure that this satisfies the standard of consent under the GDPR.

For further guidance on this the 'lawfulness, fairness and transparency' principle including consent please refer to Data Protection Policy Guidance.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data must only be processed for limited purposes. This means that Functional Areas must ensure that:

- They are only collecting the personal data for specified and legitimate purposes.
- It is made clear to individuals for what purposes their data may be used.
- Personal data are not used for purposes outside of the original purposes or in a manner which is incompatible with those purposes.
- If they wish to use personal data for any other reason, the consent of the individual must be obtained and they must be fully informed of the purposes for which it is being used.
- Personal data must not be shared or disclosed to a third party except where it relates to the purpose it was obtained, or unless a relevant exemption within data protection law applies e.g.) for the prevention, investigation, detection or prosecution of criminal offences.
    - Perform periodic reviews and maintain a record of checks carried out to ensure that personal data is collected for specified, explicit and legitimate purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Functional Areas must be clear about why they are holding personal data, be transparent when collecting personal data and only gather the necessary amount of information required from individuals to fulfil the business purpose.

- Functional Areas must perform periodic reviews and maintain a record of checks carried out to ensure that the personal data they collect is adequate, relevant and limited to what is necessary.

(d) Accurate and, where necessary, kept up to date.

- Functional Areas must have adequate procedures in place to ensure the personal data remains accurate and kept up to date where necessary.
- Every reasonable step should be taken to ensure personal data which is inaccurate are rectified or deleted.
- Functional Areas must implement procedures for complying with requests from individuals to have their data rectified without undue delay.
- Functional Areas must perform periodic reviews and maintain a record of checks carried out to ensure that personal data is accurate and, where necessary, kept up to date.

(e) Kept for no longer than necessary.

The GDPR requires the period for which personal data is retained should be kept to a strict minimum. In order to comply with this requirement:

- Functional Areas should have defined procedures in place to manage the retention, deletion or purging of information, both within TU Dublin – City Campus and with any third party who processes personal data on behalf of TU Dublin – City Campus.
- Functional Areas should only retain personal data in accordance with the TU Dublin – City Campus Data Retention Policy.

Functional Areas must perform periodic reviews and maintain a record of checks carried out to ensure that personal data is kept for no longer than necessary.

(f) Processed in a manner that ensure appropriate security of the personal data.

Functional Areas must:

- Process personal data in a manner that ensures appropriate security and confidentiality of the personal data, including preventing unauthorised access to or use of personal data and the equipment used for the processing.
- Preserve the availability, confidentiality and integrity of personal data processed in line with the TU Dublin – City Campus Information Security Policy.
- Know where they store personal data, and ensure that access to the personal data is only being available to those who require access to it as part of their role.
- Have adequate controls in place to protect the personal data during the collection, processing, storage and transmission and use only vendors approved by TU Dublin – City Campus ICT Services.
- Ensure that in the event of a systems failure; personal data is backed up and retrievable.
- Perform periodic security reviews and maintain a record of checks carried out to ensure that personal data is kept secure.

(g) Be able to demonstrate compliance with the principles.

Data Protection contains a requirement for organisations to be accountable for the way in which they process personal data and to be able to show how TU Dublin – City Campus comply with the principles. This will require Functional Areas to:

- Implement processes and procedures to support compliance. Procedures have to be put in place to support each of the minimum requirements of this Policy.
- Perform periodical monitoring and review to ensure processes and procedures are being adhered to.

Appendix 2. Key Definitions and Abbreviations

Key definitions

'Biometric data' means personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or finger prints.

'Binding Corporate Rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

'Consent' for processing is any unambiguous, freely given, specific and informed indication of a person's agreement to allow their Personal Data to be processed. To be effective individuals consent must be given by a clear affirmative action, signifying their agreement to the processing of personal data relating to him or her. Silence or pre-ticked boxes will not constitute consent.

'Cross-border processing' means either:

1) Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

2) Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."

'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

'Data Controller' is an organisation which who alone or jointly with others, determines the purposes and means of the processing of personal data.

'Data' means information in a form, which can be processed, it includes both:

- Manual Data – Information that is kept as part of a filing system, or with the intention it should be part of a relevant filing system;
- Automated Data - Information held on a computer, or recorded with the intention of putting it on a computer.

'Data Processor' means an organisation, which processes personal data on behalf of the controller.

'Data sharing agreements' set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations.

'Direct Marketing Consent and Opt -In/Out' the basic rule that applies to directing marketing is that you need the consent of the individual to use their Personal Data for direct marketing purposes. Opt-in means you can only market an individual where you have their explicit consent to do so through a medium, which they agree to i.e. email, SMS etc. A soft opt-in is when TU Dublin – City Campus can contact an existing individual about TU Dublin – City Campus's products and services where:

1. It is of a kind similar to which you sold the customer at the time you obtained their contact details
2. The individual was offered an opt-out at the time they provided their details and declined
3. Each time you send a marketing message, you give the customer the right to object to receipt of further messages
4. The sale of the product or service occurred not more than twelve months prior to the sending of the electronic marketing communication (email, SMS text message, phone etc.) or, where

applicable, the contact details were used for sending an electronic marketing communication in that twelve-month period.

Opt- out means that you have previously given them the option not to receive such marketing and they have not availed of this option.

'Functional Area' means a segment of TU Dublin – City Campus representing a specific function.

'Joint data controllers' where two or more controllers jointly determine the purposes and means of processing.

'Natural person' is a living individual. Although other laws may apply, the GDPR does not apply to deceased persons.

'Near miss' is an incident or a data breach that is unlikely to result in a risk to the individual(s) and the privacy of their data.

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular reference to 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 natural person.

'Privacy' is the right to control access to his or her personal data.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not, by automated means, such as collection, recording, organisation structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction erasure or destruction.

'**Profiling**' any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.

'Pseudonymisation' is the processing of masking personal data so that is can no longer identify an individual without the use of additional information. The data will only be pseudoanonymised provided that the additional information is kept separately and is kept secure so that the data cannot identify the individual.

'Recipient' means an organisation to whom personal data is disclosed.

'Record' is a piece of data set down in writing or some other permanent form for reference at a later stage.

'Records Management' Is the application of controls to the creation, maintenance, use and disposal of all formats of records which includes correspondence and forms, records classification, files, identification of staff member responsible for the record, retention scheduling, disaster planning, vital records protection, record conversion programmes, archival preservation activities and appropriate destruction of records.

'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.

'Special categories data' (sensitive personal data) means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural persona, data concerning health or data concerning a natural person's sex life or sexual orientation.

'Supervisory Authority' is the data protection Supervisory Authority in the state where the main establishment is.

'Third party' means an organisation or party other than the data subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

'**Withdrawing or revoking consent**' further to the above definition, this is where an individual withdraws their consent for the processing of their Personal Data by TU Dublin – City Campus.

Key abbreviations

'DP' - Data Protection

'DPIA' - Data Protection Impact Assessment

'DPO' - Data Protection Officer

'IGO' – Information Governance Officer

'DSAR' - Data Subject Access Request

'EEA' - European Economic Area

'FOI' - Freedom of Information

'GDPR' - General Data Protection Regulation

'ODPC' - Office of the Data Protection Commissioner

'SLT' - Senior Leadership Team