GDPR Common Terms and Definitions

Anonymised	Means the process of making Personal Data Anonymous Data. "Anonymised" should be construed accordingly.
Breach Incident	A breach incident includes but is not restricted to the following: • **Unauthorised disclosure** of personal data (this includes disclosure to recipients that are not authorized to receive the data) • **Loss** or theft of confidential or sensitive personal data or the equipment used to store the data (e.g. laptop, USB key, tablet, paper record) • **Accidental or unlawful destruction** (e.g. failure of equipment) • Unauthorised use of access to or **modification / alteration** of personal data or IT systems • Attempts to gain unauthorised access to information or IT systems • Human error
Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to the University, eg Strategic Plans or Intellectual Property.
Consent	Means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her. In this context, "signifies" means that there must be some active communication between the parties. Thus, a mere non-response to a communication from the University cannot constitute Consent.
Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.

Data	As used in the University's suite of Data Protection Policies, shall mean information which either: - is processed by means of equipment operating automatically in response to instructions given for that purpose; - is recorded with the intention that it should be processed by means of such equipment; - is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; - does not fall within any of the above, but forms part of a Readily Accessible record. - Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Classification	A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately or data being lost. The resulting data classification needs to be applied when handling data. It is the responsibility of data owners to classify the data under their control.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. A Data Controller can be the Sole Data Controller or a Joint Data Controller with another person or organisation or a Separate Data Controller.
Data Ownership	A process whereby information/data is assigned an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature.
Data Processor	Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within an University which is Processing Personal Data for the University as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor. It is possible for one University or person to be both a Data Controller and a Data Processor, in respect of

	distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the University is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Data Protection Commissioner	Means the Office of the Data Protection Commissioner (DPC) in Ireland.
Data Subject	Refers to the individual to whom Personal Data held relates, including employees, students, customers, suppliers.
Damage	Where the personal data has been altered, corrupted, or is no longer complete.
Destruction	Where the personal data no longer exists, or no longer exists in a form that is of any use to the Data Controller.
EEA	European Economic Area – means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
Encryption	The process of encoding information stored on a device that can add a further layer of security. It is considered an essential security measure where Personal Data is stored on a portable device or transmitted over a public network.
GDPR (General Data Protection Regulations)	Means EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data.
Loss	Where the personal data may still exist, but the Data Controller has lost control of or access to it, or no longer has the data in its possession.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title and description,

	• Tags and categories, • Who created and when, • Who last modified and when, • Who can access or update.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by TU Dublin (the University). Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of a student file or an employee HR file • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour and discipline.
Personal Data Breach	In Article 4(12) of GDPR, a "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."
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. The terms "Process" and "Processed" should be construed accordingly.
Pseudonymisation	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributable to an identified or identifiable natural person.
Records	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Record (Data) Retention Schedule	The maximum period of time information (data) should be retained by the University for legal and business purposes. It is the responsibility of data owners to define the retention period for the records/data under their control and the eventual fate of those records/data on completion of the defined period of retention.
Sensitive Personal Data	Sensitive Personal Data (or Special Category Personal Data) relates to specific categories of data which are defined as 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.
Strictly Confidential Data	Data covered by GDPR under the category of Sensitive Category Personal Data or special categories of Personal Data. If this data were to be disclosed to an unauthorised party, it could result in the loss of public confidence, non-compliance with regulations, legal liabilities and/or additional costs. Sensitive Category Personal Data under GDPR includes health data.
Third Party	Means an entity, whether or not affiliated with the University, that is in a business arrangement with the University by contract, or otherwise, that warrants ongoing risk management. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where the University has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data.
Types of Breach	**Confidentiality Breach** – where personal data is disclosed or accessed in an unauthorised or accidental manner. **Integrity Breach** – where personal data is altered in an unauthorised or accidental manner.

	Availability Breach – where personal data is lost or destroyed in an unauthorised or accidental manner.
Unauthorised or unlawful processing	This may include disclosure of personal data to (or access to) recipients who are not authorised or do not have a lawful basis to have access to the personal data.

All other terms used in the Data Protection Policies not referenced in this document, shall have the same meaning as the GDPR and/or local requirements.