Data Processing Agreement

This **Data Processing Agreement** is made the TBA

BETWEEN:

(1) **XX** a company organised and existing under the laws of Ireland, having its principal place of business located at XX, IRELAND (the **"Joint Data Controller/Processer"**); and

(2) **Technological University Dublin** a Statutory Body constituted under the Technological Universities Act 2018 and established by S.I. No. 437 of 2018, organised and existing under the laws of Ireland, having its principal place of business located at TU Dublin, Park House, Grangegorman, 191 North Circular Road, Dublin 7, D07 EWV4, Ireland] (the **"Joint Data Controller/ Processer"**)

(together the **"Parties"** and the **"Party"** shall be construed accordingly).

Recitals

A. The Data Controller acts as the data controller of the personal data relating to students registered at TU Dublin on their joint Programmes (**"Relevant Data"**).

B. The Data Processor will, from time to time, process Relevant Data on behalf of the Data Controller to enable the Data Processor to provide services to the Data Controller in accordance with the Agreement between the parties.

C. The Data Processors are also Data Controllers under this agreement as it collects additional personal data relating to students, in order to meet its legal requirements as a Designated Awarding Body and will have the full data protection obligations specified in Clause 3 in this regard.

D. All contract Parties will be Data Controllers in respect of personal data relating to students that each recruits and registers where they then forward this data on to one or all of the other contract Parties. All Parties will be Data Processors in respect of personal data relating to students that is made available to them by a Data Controller.

1. Definitions

Words and expressions used in this Agreement but not defined herein shall have the meanings given to such words and expressions in the EU Directive 95/46/EC or, from 25 May 2018, the General Data Protection Regulation (2016/679) (**"Applicable Data Protection Law"**).

2. Details of the Processing Operations

The subject matter of the processing, including the processing operations carried out by the Data Processor on behalf of the Data Controller and the instructions of the Data Controller to the Data Processor, are described in **Schedule A**, which forms an integral part of this Agreement. The Data Processor acts on behalf of and on the instructions of the Data Controller in carrying out the processing operations.

3. Obligations of the Data Controller

3.1. The Data Controller determines the purposes for which Relevant Data are or will be processed, and the manner in which they are or will be processed.

3.2. The Data Controller agrees and confirms that:

3.2.1. it has taken measures concerning the Relevant Data to ensure compliance with its personal data security and other obligations prescribed by Applicable Data Protection Law for data controllers;

3.2.2. it has taken measures to establish a procedure for the exercise of the rights of the individuals whose Relevant Data are collected;

3.2.3. it only processes Relevant Data that have been lawfully and validly collected and that such data will be relevant and proportionate to the respective uses;

3.2.4. after assessment of the requirements of Applicable Data Protection Law, the security and confidentiality measures implemented for the Relevant Data are reasonably suitable for protection of the Relevant Data against any accidental or unlawful destruction, accidental loss, alteration, unauthorised or unlawful disclosure or access, in particular when the processing involves data transmission over a network, and against any other forms of unlawful or unauthorised processing; and

3.2.5. it will take reasonable steps to ensure compliance with the provisions of this Agreement by its personnel and by any person accessing or using Relevant Data on its behalf.

4. Obligations of the Data Processor

4.1. The Data Processor carries out the processing of Relevant Data on behalf of the Data Controller.

4.2. In discharging its obligations under the Agreement and this Data Sharing Agreement, the parties are responsible for compliance with all applicable data protection or privacy legislation and will ensure that all necessary registrations and notifications are made and provide the other party with a copy, on request, of evidence of such and evidence of any amendments or alterations made thereto.

4.3. Without prejudice to the generality of clause 4.2 and further to the provisions of Article 28 of the GDPR, the Data Processor agrees that it will:

4.3.1. process Relevant Data only on behalf of the Data Controller and in compliance with the Data Controller's instructions (including relating to international data transfers), this Data Sharing Agreement and the Agreement and shall not disclose Relevant Data to any third party (including for back-up purposes) apart from the sub-processors authorised by the Data Controller under this Data Sharing Agreement, and which are listed in **Schedule B**. If the Data Processor cannot provide such compliance, it shall promptly inform the Data Controller of its inability to comply in which case the Data Controller is entitled to immediately terminate the Agreement and this Data Sharing Agreement and the Data Processor's access to Relevant Data and/or to take any other reasonable action;

4.3.2. if in the Data Processor's opinion an instruction from the Data Controller infringes Applicable Data Protection Law, immediately inform the Data Controller;

4.3.3. implement the technical and organisational security measures provided for in **Schedule C** prior to the launch of the processing activities for the Relevant Data and provide the Data Controller with copies of its privacy and security policies;

4.3.4. take all reasonable steps to ensure that (i) persons employed by it; and (ii) other persons engaged at its place of business, who process Relevant Data, are aware of, and comply with this Data Sharing Agreement; and that there is a Data Protection Officer whose primary concern is enabling compliance with the GDPR;

4.3.5. comply with strict confidentiality obligations in respect of the Relevant Data and ensure that its employees, authorised agents and any sub-processors are legally required in writing to comply with and acknowledge and respect the confidentiality of the Relevant Data, including after the end of their employment, contract or at the end of their assignment;

4.3.6. inform the Data Controller without delay of:

4.3.6.1. any non-compliance by the Data Processor or its employees with this Data Sharing Agreement or the regulatory provisions relating to the protection of Relevant Data processed under this Data Sharing Agreement;

4.3.6.2. any legally binding request for disclosure of Relevant Data by a law enforcement authority, unless otherwise prohibited, such as in order to preserve the confidentiality of an investigation by the law enforcement authorities;

4.3.6.3. any incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alternation of Relevant Data;

4.3.6.4. any notice, inquiry or investigation by a supervisory authority; and

4.3.6.5. any complaint, inquiry or request (in particular, requests for access to, rectification or blocking of Relevant Data) received directly from the data subjects without responding to that request, unless the Data Controller has authorised a response;

4.3.7. to fully co-operate with and assist the Data Controller without delay in respect of the Data Controller's obligations regarding:

4.3.7.1. requests from data subjects in respect of access to or the rectification, erasure, restriction, blocking or deletion of Relevant Data. In the event that a data subject sends such a request directly to the Data Processor, the Data Processor will pass it on to the Data Controller without delay;

4.3.7.2. the investigation of any incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alternation of Relevant Data and the notification to the supervisory authority and data subjects in respect of such incidents;

4.3.7.3. the preparation of data protection impact assessments and, where applicable, carrying out consultations with the supervisory authority;

4.3.7.4. the security of Relevant Data, including by implementing the technical and organisational security measures provided for in Schedule C;

4.3.8. if the Data Processor is required by law to process Relevant Data, inform the Data Controller of this requirement in advance of any processing, unless the Data Processor is prohibited from informing the Data Controller on grounds of important public interest; and

4.3.9. make available to the Data Controller all information necessary to demonstrate compliance with the obligations in this Clause 4.

4.4. **Audit:** Both parties agree, at the request of the other, to submit its data processing facilities and/or any location from which Relevant Data can be accessed for audit to ascertain and/or monitor compliance with this Data Sharing Agreement, the GDPR and any other applicable data protection or privacy law generally which audit shall be carried out, with reasonable notice and during regular business hours and under a duty of confidentiality, by the party and/or by a third party appointed by them. [Both parties shall indemnify against all damage liability and harm of

every description which may arise whether directly or indirectly in consequence of the processing of the Relevant Data and/or the performance or non-performance under the Agreement. This provision shall survive the termination or expiry of this Agreement].

5. Prohibition on transfer and disclosure

5.1. The Data Processor agrees, if it intends to engage one or more third parties acting on its behalf to help it to satisfy its obligations in accordance with this Data Sharing Agreement and to delegate all or part of the processing activities to such sub-processors to obtain the prior written consent of the Data Controller to the subcontracting, such consent not to be unreasonably withheld. The Data Processor shall enter into contractual arrangements with such approved sub-processors requiring them to guarantee a similar level of data protection compliance and information security to that provided for herein. If a sub-processor fails to comply with its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance (or failure of performance) of the sub-processor's data protection obligations.

5.2. To the maximum extent permitted by applicable law and without prejudice to the generality of clauses 4 or 5.1, without the prior written consent of the Data Controller, the Data Processor shall not:

5.2.1. disclose Relevant Data to any third party, including, without limitation, any law enforcement or governmental authority; or

5.2.2. transfer Relevant Data outside the European Economic Area or a country approved by the European Commission pursuant to Article 25(6) of Directive 95/46/EC or, as applicable, Article 45(1) of the GDPR.

6. Post-termination obligations

The Parties agree that on the termination of the data processing services, the Data Processor and any sub-processors may, with the agreement of the Data Controller, retain certain Relevant Data for verification of award purposes only and shall, at the choice of the Data Controller, return all other Relevant Data and copies of such data to the Data Controller or securely destroy them and demonstrate to the satisfaction of the Data Controller that it has taken such measures, unless applicable EU or EU member state law prevents it from returning or destroying all or part of the Relevant Data disclosed. In such case, the Data Processor or sub-processor agree to preserve the confidentiality of the Relevant Data retained by it and that it will only actively process such Relevant Data after such date in order to comply with the laws it is subject to.

7. Transferring this Data Sharing Agreement

The Data Sharing Agreement is personal to the Data Processor and the Data Processor shall not assign or transfer any of its rights or obligations under the Data Sharing Agreement without the Data Controller's prior written consent.

8. Insurance

The parties shall effect and maintain at its own cost policies of insurance for any occurrence or series of occurrences arising out of any one event arising out of the performance of its obligations under this Data Sharing Agreement. Upon request, the parties shall provide the other with a copy of the policy of insurance affected in accordance with this clause 8.

9. Governing law and jurisdiction

9.1. This Data Sharing Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the law of Ireland.

9.2. The parties to this Data Sharing Agreement irrevocably agree that the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Data Sharing Agreement or its subject matter or formation (including non-contractual disputes or claims).

Signature: _____

Name:

Title:

For and on behalf of the XX

Signature: _____

Name:

Title:

For and on behalf of TU Dublin

Signature: _____

Name:

Title:

For and on behalf of TU Dublin

Schedule A

Details of the Processing Activities (to be confirmed by both Parties)
to be read in conjunction with overall Agreement between the Parties

Data subjects

The personal data comprises the following categories of data subjects:

- Current, past and prospective students who apply to or are registered on the **joint programmes**
- Staff involved in the administration, management and delivery of the **joint programmes**

Categories of data

The personal data includes but is not limited to the following:

First Name
Middle Name (if applicable)
Last Name
Prefix
PPS Number
Date of birth (dd-mm-yyyy format)
Gender
Email address (personal email)
Contact phone number
Home Address
Nation of Birth
Nation of Citizenship
Domiciliary (i.e. country in which the student lived for the last 12 months prior to registering on the programme – this may differ from citizenship)
Programme Code
Educational Record
Assessment Material and Results
Photograph
Application Details and Documents

Special categories of data

The personal data may include the following special categories of data:
Ethnic background

Processing activities

The personal data may be subject to the following processing activities:

A. Hosting of the collected data.
B. Use of personal data for purpose of communication with the data subject
C. Use of personal data to enable the parties to fulfil its obligations under the Agreement to deliver the programme and to record and disseminate results from the programme
D. Use of personal data so that the parties may fulfil its statutory reporting obligations

Legal Basis for Processing the Data is :

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Data Retention Period

The Data is retained in **TU Dublin** accordance with the **TU Dublin Data Retention Policy** and in **XX** by the **XX Data Retention Policy**

Schedule B

Sub-processors processing Controller Data under this Data Sharing Agreement

Sub-processor Name: **Sub-processor Address:** **Will Relevant Data be subject to International Transfers by this Sub-processor, as outlined in Clause 5.2?**
Sub-processor Name: Microsoft **Sub-processor Address:** One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521 **Will Relevant Data be subject to International Transfers by this Sub-processor, as outlined in Clause 5.2?** Yes
Sub-processor Name: **Sub-processor Address:** **Will Relevant Data be subject to International Transfers by this Sub-processor, as outlined in Clause 5.2?** **Yes / No**
(Add additional sub-processors as required)

Schedule C

Technical and Organisational Security Measures

1.1 In accordance with Clause 4 of the Data Sharing Agreement, the Data Processor will adopt and maintain appropriate (including organisational and technical) security measures in dealing with the Relevant Data in order to protect against unauthorised or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In determining the technical and organisational security measures required in Clause 4 of the Data Sharing Agreement, the Data Processor will take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Data Processor will implement the following specific security measures in respect of the Relevant Data, as applicable:

(a) the ability to ensure ongoing confidentiality, integrity, availability and resilience of its processing systems and the Services. This shall include a process to ensure corporate systems and databases are protected from unauthorised access, are password protected, and regularly updated with security patches; and that remote access to the Processor's Data Centre(s) requires multi-factor authentication over a secure VPN connection

(b) all data transfers to and from the Processor's Data Centre(s) are encrypted via SSL/TLS connections

(c) a process to log all access to and use of the Relevant Data and make such logs available to the Data Controller without delay upon request

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

(e) a process for preventing unauthorised persons from gaining access to Controller Data and ensuring that only appropriately trained and authorised employees, Sub-Processors, agents and/or contractors have access limited to such parts of Controller Data as is necessary for performance of Data Processor's duties;

(f) a process for preserving, so far as possible, the integrity of Controller Data and prevent any loss, unauthorised disclosure, duplication, theft, manipulation or interception of or degradation in Controller Data;

(g) a process for making secure back-up copies of Controller Data on such regular basis as is reasonable for the particular data concerned as required by the Processor's disaster recovery and business continuity plan to ensure that availability and access to Controller Data can be restored in a timely manner in the event of a physical or technical incident; and

(together the "Security Measures")

1.1.2 The Processor shall ensure that it at all times complies with the Security Measures and shall not implement any proposed changes to the Security Measures which would adversely affect the security of Controller Data unless previously agreed in writing by the Controller.

1.1.3 The Processor shall and shall procure that its Sub-Processors shall, notify the Controller promptly and without undue delay (and in any event within 48 hours) of any

actual, anticipated or suspected Security Breach and promptly take reasonable steps to minimise harm and secure the Controller Data.

1.1.4 In the event that Controller Data is corrupted or lost or sufficiently degraded as to be unusable, the Controller shall have the option to require the Processor, at the processor's own expense, to restore or procure the restoration of Controller Data to the Controller's satisfaction.