

SCHEDULE 2*(Revised May 2023)***DATA PROTECTION**

This Schedule forms part of the Approved International Student Recruitment Counsellor Agreement (the Counsellor Agreement) between INTO and the Counsellor to reflect the Parties' agreement with regard to the Processing of Personal Data.

In this Schedule, the following words and expressions shall have the following meanings:

"Applicable Laws"	means any and all applicable provisions of statutes, laws, rules, codes, treaties, ordinances, decisions, directions, injunctions, awards or regulations, including from any court or any regulatory or governmental authority in any jurisdiction which are relevant to the activities envisaged under the Counsellor Agreement;
"Controller", "Data Subject", "Processing" and "Processor"	shall have the meanings given to those terms in the Data Protection Laws, and "Process" and "Processed" shall be construed accordingly;
"Data Protection Impact Assessment"	means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the GDPR;
"Data Protection Laws"	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time to which a Party is subject, including a) the UK GDPR and the Data Protection Act 2018; and (b) to the extent the EU GDPR applies, the law of the European Union or any member state to which the Counsellor is subject, which relates to the protection of personal data; and (c) any code of practice or guidance published by a Regulator from time to time;
"Data Protection Particulars"	means, in relation to any Processing under the Counsellor Agreement: the subject matter and duration of the Processing; the nature and purpose of the Processing; the type of Personal Data being Processed; and the categories of Data Subjects;
"Data Subject Request"	means an actual or purported request or notice or complaint from or on behalf of a Data Subject exercising his rights under the Data Protection Laws in relation to Personal Data including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object;
"European Union"	means the European Union as it is made up from time to time;
"EU GDPR"	means Regulation (EU) 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 repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1, 4.5.2016;
"Good Industry Practice"	means, at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of similar services as those provided under this Agreement, such supplier seeking to comply with its contractual obligations in full and complying with all applicable laws (including the Data Protection Laws);

"ICO"	means the UK Information Commissioner's Office, or any successor or replacement body from time to time;
"Personal Data"	has the meaning set out in the Data Protection Laws and for the purposes of the Counsellor Agreement includes Special Categories of Personal Data;
"Personal Data Breach"	has the meaning set out in the Data Protection Laws and, for the avoidance of doubt, includes a breach of Paragraphs 1.6 and/or 2.3.4;
"Regulator"	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws, including without limitation (where applicable) in the UK, the ICO;
"Regulator Correspondence"	means any correspondence from a Regulator in relation to the Processing of Student Data;
"Restricted Country"	means a country, territory or jurisdiction outside of a) the UK which the UK government has not deemed to provide adequate protection in accordance with Article 45(1) of the UK GDPR or b) the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 45(1) of the EU GDPR (as applicable);
"Security Requirements"	means the requirements regarding the security of Personal Data, asset out in the Data Protection Laws (including, in particular and as appropriate, the measures set out in Article 32(1) of the UK GDPR (taking due account of the matters described in Article 32(2) of the UK GDPR)) and as otherwise agreed by the Parties from time to time;
"Student Data"	any Personal Data relating to Students;
"Third Party Request"	means a written request from any third party for disclosure of Student Data where compliance with such request is required or purported to be required by law.
"UK GDPR"	means the EU GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).

1. Arrangement Between The Parties

- 1.1 The Parties shall each Process the Student Data and acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Laws.
- 1.2 Notwithstanding Paragraph 1.1 the Parties anticipate that:
- 1.2.1 INTO shall be a Controller where it is Processing the Student Data for the purposes of assessing Student applications and issuing offers of places in respect of Programmes of the INTO JVs and the INTO Subsidiaries and assessing applications in respect of the Direct Entry Programmes; the relevant INTO JV and INTO Subsidiary shall be a Controller where it is Processing the Student Data in relation to its recruitment of Students to, and provision of, its respective Programmes; and the relevant INTO Partner University shall be a Controller where it is Processing the Student Data in relation to the recruitment of Students to, and the provision of, its own programmes, including Direct Entry Programmes; and
- 1.2.2 The Counsellor shall be a Controller where it is Processing the Student Data on its own behalf and determines the purposes for which and the manner in which any such Student Data are, or are to be, Processed.

- 1.3 Each of the Parties acknowledges and agrees that Appendix 1 (*Data Protection Particulars*) to this Schedule 2 is an accurate description of the Data Protection Particulars;
- 1.4 The Counsellor undertakes to comply with the terms of this Schedule and the Data Protection Laws in Processing the Student Data and undertakes to ensure that:
 - 1.4.1 it is not subject to any prohibition or restriction which would prevent or restrict it from disclosing or transferring the Student Data to INTO or to INTO providing the Student Data to the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University in accordance with the terms of the Counsellor Agreement;
 - 1.4.2 all fair processing notices (as required under Data Protection Laws) have been given (and/or, as applicable, consents obtained), including in relation to any Personal Data, and are sufficient in scope to:
 - (i) allow INTO, the relevant INTO JV, the relevant INTO Subsidiary and the relevant INTO Partner University to access and Process the Student Data as required and envisaged under the Counsellor Agreement;
 - (ii) disclose or transfer the Student Data (or relevant Student Data as applicable) to other third parties in accordance with the terms of the Counsellor Agreement.;
 - 1.4.3 all Student Data disclosed or transferred to, or accessed by INTO, the relevant INTO JV, the relevant INTO Subsidiary and the relevant INTO Partner University is accurate and up-to-date, adequate, relevant and not excessive to enable INTO, the relevant INTO JV, the relevant INTO Subsidiary and the relevant INTO Partner University to Process the Student Data as envisaged under the Counsellor Agreement.
- 1.5 Without limitation to its obligations under Paragraph 1.4 the Counsellor undertakes to obtain the written consent of Students, in a form acceptable to INTO for the collection and export and transfer of their Personal Data to INTO, the relevant INTO JV, the relevant INTO Subsidiary and the relevant INTO Partner University and the Processing of such Personal Data in accordance with the terms of the Counsellor Agreement.
- 1.6 The Counsellor shall ensure that in Processing the Student Data and supplying it to INTO and, if required by INTO, to the relevant INTO JV, the relevant INTO Subsidiary and the relevant INTO Partner University, appropriate technical and organisational security measures are in place sufficient to comply with at least the Security Requirements and where requested by INTO provide evidence of its compliance with such requirements promptly and in any event within forty-eight (48) hours of the request.
- 1.7 The Counsellor shall notify INTO promptly and in any event within forty-eight hours of receipt of any Data Subject Request or Regulator Correspondence which relates directly or indirectly to the Processing of Student Data under, or in connection with, the Counsellor Agreement and together with such notice, provide a copy of such Data Subject Request or Regulator Correspondence to INTO and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 1.7, the Counsellor shall provide INTO with all reasonable co-operation and assistance required by INTO in relation to any such Data Subject Request or Regulator Correspondence.
- 1.8 The Counsellor shall use reasonable endeavours to notify INTO if it is obliged to make a disclosure of any of the Student Data Processed under or in connection with the Counsellor Agreement under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless the Counsellor is prohibited from doing so by law.
- 1.9 The Counsellor shall take reasonable steps to ensure the reliability of any of its personnel who have access to the Student Data Processed under or in connection with the Counsellor Agreement.
- 1.10 The Counsellor shall hold the information contained in the Student Data Processed under or in connection with the Counsellor Agreement confidentially and under at least the conditions of confidence as it holds Personal Data Processed by it other than such Student Data.
- 1.11 For the avoidance of doubt, the Parties agree that any Student Data or other Personal Data collected by the Counsellor on its own behalf and for its own purposes independently of INTO will not be subject to Paragraph 2 below.

- 1.12 Where any Party is deemed to be a joint Controller with another in relation to the Student Data, the Parties shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and shall co-operate to do all necessary things to enable performance of such compliance obligations, save that each Party shall be responsible, without limitation, for compliance with its data security obligations equivalent to those set out in Paragraph 2.3.4 where Student Data has been transmitted by it, or while Student Data is in its possession or control.
- 1.13 The Parties each acknowledge and agree that they may need to Process Personal Data relating to each Party's representatives (in their respective capacities as Controllers) in order to (as appropriate):
- (a) administer and perform their respective activities and obligations under the Counsellor Agreement;
 - (b) compile, dispatch and manage the payment of any commission agreed under the Counsellor Agreement;
 - (c) manage the Counsellor Agreement and resolve any disputes relating to it;
 - (d) respond and/or raise general queries relating to the Counsellor Agreement; and
 - (e) comply with their respective regulatory obligations.
- 1.14 Each Party shall Process such Personal Data relating to each Party's representatives for the purposes set out in Paragraph 1.13 in accordance with their respective privacy policies. The Parties acknowledge that they may be required to share Personal Data with their affiliates, group companies and other relevant parties, within or outside of the country of origin, in order to carry out the activities listed in Paragraph 1.13, and in doing so each Party will ensure that the sharing and use of this Personal Data complies with applicable Data Protection Laws.

2. Processor Obligations

- 2.1 It is not anticipated that the Counsellor will Process any Student Data under the Counsellor Agreement for and on behalf of INTO as a Processor or sub-Processor appointed by INTO but in the event that the Counsellor does process any Student Data for and on behalf of INTO as a Processor or sub-Processor appointed by INTO, it shall comply with the terms of this Schedule and the Data Protection Laws in Processing the Student Data.
- 2.2 Each of the Parties acknowledges and agrees that in the event that the Counsellor Processes any Student Data for and on behalf of INTO as a Processor or sub-Processor appointed by INTO the Parties shall agree in writing the particulars of the Student Data Processing including the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data being Processed and the categories of Data Subjects.
- 2.3 To the extent that the Counsellor does act:
- (a) as a Processor for and on behalf of INTO as Controller; or
 - (b) as a sub-Processor for and on behalf of INTO acting as Processor for and on behalf of the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University as the Controller in relation to the Processing of the Student Data arising out of, or in connection with, the performance of its obligations under the Counsellor Agreement, it shall:
 - 2.3.1 Process the Student Data for and on behalf of INTO for the purposes of performing its obligations under the Counsellor Agreement and only in accordance with the terms of the Counsellor Agreement and any written instructions from INTO including complying with any systems or procedures which INTO may introduce from time to time in respect of the Processing of the Student Data;
 - 2.3.2 notify INTO immediately (and in any event within twenty-four (24) hours) if it considers, in its opinion (acting reasonably), that any of INTO's instructions under Paragraph 2.3.1 infringes any of the Data Protection Laws;
 - 2.3.3 implement appropriate operational, organisational and technical measures to ensure a level of security appropriate to the risk presented by Processing the Student Data, in particular from a Personal Data Breach and to safeguard against any unauthorised or unlawful Processing of the Student Data and against accidental or unlawful loss or alteration or unauthorised disclosure or destruction of, or damage or access to, Student Data, including

- implementing such physical and/or technical security obligations as are required by INTO from time to time and where requested provide to INTO evidence of its compliance with such requirement;
- 2.3.4 take all reasonable steps to ensure the reliability and integrity of all of its staff who shall have access to the Student Data, and ensure that each member of its staff shall receive training in the handling of Student Data and have entered into appropriate contractually-binding confidentiality undertakings in relation to the Student Data;
- 2.3.5 make available to INTO all information necessary to demonstrate compliance with the obligations laid down in Data Protection Laws and allow for and contribute to audits, including inspections, conducted by INTO or another auditor mandated by INTO and allow its data Processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by INTO (and/or their representatives, including their appointed auditors) in order to ascertain compliance with the terms of this Schedule 2 (*Data Protection*), and provide reasonable information, assistance and co-operation to INTO, including access to relevant staff and/or, on the request of INTO, provide INTO (as appropriate), with written evidence of its compliance with the requirements of this Schedule 2 (*Data Protection*);
- 2.3.6 keep the Student Data confidential and not disclose Student Data to a third party (including a sub-contractor, sub-Processor or sub-agent) in any circumstances without INTO's prior written consent and PROVIDED ALWAYS that any such consent shall be subject to the Counsellor:
- (a) undertaking thorough due diligence on the proposed sub-contractor (or sub-Processor or sub-agent), including a risk assessment of the information governance-related practices and processes of the proposed sub-contractor (or sub-Processor or sub-agent), which shall be used by the Counsellor to inform any decision on appointing the proposed sub-contractor (or sub-Processor or sub-agent);
 - (b) providing INTO with full details of the proposed sub-contractor (or sub-Processor or sub-agent) (including the results of the due diligence undertaken in accordance with Paragraph 2.3.7(a)) before its appointment and INTO has consented to such appointment in writing;
 - (c) ensuring that the sub-contractor (or sub-Processor or sub-agent) contract (as it relates to the Processing of Personal Data) is on terms which are the same as, and in any case no less onerous than, the terms set out in this Paragraph 2.3. and which ensure that the sub-contractor's (or sub-Processor's or sub-agent's) right to Process the Student Data terminates automatically on expiry or termination of the Counsellor Agreement for whatever reason; and
 - (d) remaining primarily liable to INTO for the acts, errors and omissions of any sub-contractor (or sub-Processor or sub-agent) to whom it discloses Student Data, and shall be responsible to INTO for the acts, errors and omissions of such sub-contractor (or sub-Processor or sub-agent) as if they were the Counsellor's own acts, errors and omissions to the extent that the Counsellor would be liable to INTO under the Counsellor Agreement for those acts, errors and omissions;
- 2.3.7 without limitation to Paragraph 3 not transfer any Student Data to a Restricted Country (save for transfer to INTO, or if required by INTO to the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University as appropriate) except with the prior written consent of INTO and in granting consent to the transfer, INTO may impose such terms as INTO considers appropriate on the Processing of the Student Data by the Counsellor, including entering into the standard contractual clauses (SCCs) (as referred to in Paragraph 3) and/or a direct Data Processing Agreement with the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University;
- 2.3.8 notify INTO promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or Regulator Correspondence or Third Party Request, and shall:
- (a) not disclose any Student Data in response to any Data Subject Request or Regulator Correspondence or Third Party Request without INTO's prior written consent; and
 - (b) promptly and in any event in accordance with the instructions of INTO provide INTO with all reasonable co-operation and assistance required by INTO in relation to any such Data Subject Request or Regulator Correspondence or Third Party Request to

- enable INTO to comply with the relevant timescales set out in the Data Protection Laws; and
- (c) provide INTO with all reasonable co-operation and assistance in complying with any Data Subject Request, and/or responding to any enquiry made, or investigation or assessment of Processing initiated by a Regulator in respect of the Student Data and will not respond directly to any such request or enquiry.
- 2.3.9 notify INTO promptly (and in any event within twenty-four (24) hours) upon reasonably suspecting and/or becoming aware of any actual or suspected, threatened or 'near miss' Personal Data Breach and:
- (a) provide INTO with all material information in its possession reasonably required by INTO to comply with the informal or formal security breach management and reporting obligations recommended or required by the Regulator from time to time concerning any Personal Data Breach (including: the type of Personal Data/information involved; number of records involved/people affected; circumstances of breach; mitigation and actions taken; investigation details; details of reports to and reactions from other relevant bodies of the breach);
- (b) implement any measures necessary to restore the security of compromised Student Data;
- (c) assist INTO to make any notifications to the Regulator and affected Data Subjects and comply with its obligations in relation to Personal Data Breaches under Data Protection Laws ; and
- (d) not make any announcement or publish or otherwise authorise any broadcast of any notice or information about a Personal Data Breach without the prior written consent of and prior written approval of INTO of the content, media and timing of any such notice or information (save to the extent required by the law applicable to the Counsellor).
- 2.3.10 except to the extent required by law (being the governing law of the Counsellor Agreement) or otherwise as applicable in relation to the legal obligations of each Party, on termination or expiry of the Counsellor Agreement (as applicable) cease Processing all Student Data Processed on behalf of INTO and return and/or provide a secure copy of all such Student Data to INTO and permanently and securely destroy (as directed in writing by INTO) all such Student Data and all copies remaining in its possession or control and not retain any copy, abstract, precis or summary of any Student Data Processed on behalf of INTO;
- 2.3.11 comply with the obligations imposed upon a Processor under the Data Protection Laws and perform its obligations under the Counsellor Agreement in a manner which does not place INTO, the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University in breach of the Data Protection Laws;
- 2.3.12 use all reasonable endeavours in accordance with Good Industry Practice to assist INTO to comply with the obligations imposed on INTO by the Data Protection Laws, including:
- (a) obligations relating to ensuring the security and integrity of the Student Data;
- (b) obligations relating to notifications and communication of Personal Data Breaches required by the Data Protection Laws to the Regulator and/or any relevant Data Subjects; and
- (c) undertaking any Data Protection Impact Assessments that are required by the Data Protection Laws (and, where required by the Data Protection Laws, consulting with the Regulator in respect of any such Data Protection Impact Assessments);
- 2.3.13 not amend or delete the Student Data Processed on behalf of INTO except where instructed to do so by INTO; and
- 2.3.14 at all times comply with and support INTO in complying with any agreement between INTO and any Data Subject in relation to any Processing of Student Data including in relation to any Data Subject Request and with any Court order requiring the rectification, blocking, erasure or destruction of any Student Data notified to the Counsellor by INTO in writing from time to time.

3. UK and EEA Restricted Transfers

- 3.1 INTO acknowledges and agrees that the Counsellor may store and Process Student Data outside the UK or the EEA. The Parties agree that, to the extent INTO's transfer of Student Data to the Counsellor results in a Restricted Transfer:
- (a) in the event of a UK Restricted Transfer, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (i) varied to address the requirements of the UK GDPR in accordance with UK International Data Transfer Addendum (Appendix 2 to this Schedule); and (ii) entered into by the Parties and incorporated by reference into this DPA; and
 - (b) in the event of an EEA Restricted Transfer, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (i) the Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Controller Established in a Third Country (Controller-to-Controller Transfers) as set out in Schedule 3 to the Counsellor Agreement; and (ii) entered into by the Parties and incorporated by reference into this DPA.
4. Notwithstanding anything in the Counsellor Agreement to the contrary, this Schedule 2 (*Data Protection*) shall continue in full force and effect for so long as the Counsellor Processes any Student Data under or in connection with the Counsellor Agreement.
5. If the appropriate safeguards demonstrated or implemented by the Counsellor (or the relevant Processor) in accordance with Paragraphs 3 and/or 4 of this Schedule are deemed at any time not to provide an adequate level of protection in relation to Student Data, the Counsellor will implement such alternative measures as may be required by INTO to ensure that the relevant transfer to a Restricted Country and all resulting Processing are compliant with Data Protection Laws.
- ### **6. Change of law**
- 6.1 Upon a change in Applicable Laws, the Parties acknowledge it may be necessary to and will amend the terms of this Schedule in so far as is required to ensure the Parties continued compliance with the Data Protection Laws and/or any other Applicable Laws.

APPENDIX 1 TO SCHEDULE 2

DATA PROTECTION PARTICULARS

The subject matter and duration of the Processing	<p>INTO shall be a Controller where it is Processing the Student Data for the purposes of assessing Student applications and issuing offers of places on the Programmes at the INTO JVs and the INTO Subsidiaries or assessing applications in respect of the Direct Entry Programmes; the relevant INTO JV and INTO Subsidiary shall be a Controller where it is Processing the Student Data in relation to its recruitment of Students to, and provision of, its respective Programmes; and the relevant INTO Partner University shall be a Controller where it is Processing the Student Data in relation to the recruitment of Students to, and the provision of, its own Programmes, including Direct Entry Programmes.</p> <p>The Counsellor shall be a Controller where it is Processing the Student Data on its own behalf and determines the purposes for which and the manner in which any such Student Data is, or is to be Processed and in relation to the performance of its obligations under the Counsellor Agreement.</p> <p>The Student Data shall be Processed by the Parties for the term of this Agreement and otherwise in accordance with their respective Data Protection policies.</p>
The nature and purpose of the Processing	The recruitment of students, including the Students, to the Programmes or direct enrolment at INTO Partner Universities, and in connection with, and as is necessary for the performance of, each Party's obligations under the Counsellor Agreement.
The type of Personal Data being Processed	Name, address, date of birth, gender, nationality, email address, phone number, education history and qualification details, GPA, personal statement, photograph, copy of passport, references, portfolio, EU ID card, course information, parental consent (if Student is under 18), visa information and emergency contact details (including name, relationship to data subject and contact number), financial information and information relating to race and ethnic origin, religious beliefs, health, medical and disabilities.
The categories of Data Subjects	Students for (potential) enrolment with the relevant INTO JV, the relevant INTO Subsidiary or direct enrolment at INTO Partner Universities.

APPENDIX 2 TO SCHEDULE 2

UK International Data Transfer Addendum

Amendment to Schedule 2 of the Approved International Student Recruitment Counsellor Agreement

The entities set out below have entered into the Approved International Student Recruitment Counsellor Agreement (the Agreement).

This UK International Data Transfer Addendum (UK Addendum) amends Schedule 2 of the Approved International Student Recruitment Counsellor Agreement by modifying the EU Standard Contractual Clauses (Controller to Controller) in Schedule 3 as follows:

Effect of Amendment:

Subject to the modifications set out in this UK Addendum, the Approved International Student Recruitment Counsellor Agreement remains in full force and effect.

Part 1: Tables

Table 1: Parties

Start date	From the first date that the Counsellor provides Personal Data to INTO	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: INTO University Partnerships Limited Main address (if a company registered address): One Gloucester Place, Brighton, BN1 4AA Official registration number (if any) (company number or similar identifier): 05507863	Name of the Data Importing Organisation: "The Counsellor" Main address (if a company registered address): As set out in the Approved International Student Recruitment Counsellor Agreement Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Data Protection Officer Contact details including email: privacy@intoglobal.com	Full Name (optional): As stated in the Approved International Student Recruitment Counsellor Agreement Job Title: As stated in the Approved International Student Recruitment Counsellor Agreement Contact details including email: As stated in the Approved International Student Recruitment Counsellor Agreement
Signature (if required for the purposes of Part 2 - see below)	The Party's signature of the Counsellor Agreement shall be considered as a signature to this UK Addendum	The Party's signature of the Counsellor Agreement shall be considered as a signature to this UK Addendum

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		<p>1. <input checked="" type="checkbox"/> The version of the Approved EU SCCs which this UK Addendum is appended to in Schedule 3 of the Counsellor Agreement and as detailed below, including the Appendix Information:</p> <p>Date: Date of the Approved International Student Counsellor Agreement with The Counsellor</p> <p>Reference (if any):</p> <p>Other identifier (if any):</p> <p>Or</p> <p>2. <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Addendum:</p>				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties:

INTO University Partnerships Limited and The Counsellor

Other information to identify INTO University Partnerships Ltd:

INTO shall in relation to this UK Addendum represent and act on behalf of itself, the relevant INTO JV, the relevant INTO Subsidiary and/or the relevant INTO Partner University (each as defined in the Approved International Student Recruitment Counsellor Agreement between INTO and the Counsellor).

Annex 1B: Description of Transfer:

The Personal Data of International Students for recruitment to the Programmes or direct enrolment at INTO Partner Universities, and in connection with, and as is necessary for the performance of, each Party's obligations under the Approved International Student Recruitment Counsellor Agreement.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Each Party must apply such measures that are appropriate to the risks when transferring Personal Data, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the Processing.

Annex III: List of Sub processors (Modules 2 and 3 only):

Not applicable - it is expected that only Module 1 will be relevant for the transfer of Personal Data between the Parties.

Table 4: Ending this UK Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: <input type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	--

Part 2: Mandatory Clauses

Entering into this UK Addendum

- Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

- Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 17.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 14 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
- a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:
“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
 - c. Clause 6 (Description of the transfer(s)) is replaced with:
“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
 - d. Clause 8.7(i) of Module 1 is replaced with:
“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
 - f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;
 - h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
 - i. Reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
 - j. Clause 13(a) and Part C of Annex I are not used;
 - k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
 - l. In Clause 16(e), subsection (i) is replaced with:
“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
 - m. Clause 17 is replaced with:
“These Clauses are governed by the laws of England and Wales.”;
 - n. Clause 18 is replaced with:
“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
 - o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 17, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
- a. its direct costs of performing its obligations under the Addendum; and/or
 - b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 17 of those Mandatory Clauses.
--------------------------	---

SCHEDULE 3

(Revised May 2023)

**Standard Contractual Clauses for Personal Data Transfers from
an EU Controller to a Controller Established in a Third Country
(Controller-to-Controller Transfers)**

SECTION I

CLAUSE 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation)[FN1] for the transfer of personal data to a third country.
- (b) The Parties:
- i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each data importer)
- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - v. Clause 13;
 - vi. Clause 15.1(c), (d) and (e);
 - vii. Clause 16(e);
 - viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

CLAUSE 7 - Optional

Docking clause

N/A

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- i. where it has obtained the data subject's prior consent;
- ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
 - i. of its identity and contact details;
 - ii. of the categories of personal data processed;
 - iii. of the right to obtain a copy of these Clauses;
 - iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[FN2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[FN3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

N/A

CLAUSE 10

Data subject rights

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[FN10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge:
- i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
 - ii. rectify inaccurate or incomplete data concerning the data subject;
 - iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
- i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
 - ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the

reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

CLAUSE 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

CLAUSE 13

Supervision

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[FN12];
 - iii. any relevant contractual, technical or organisational safeguards put in place to supplement

the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if:
 - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - ii. the data importer is in substantial or persistent breach of these Clauses; or
 - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall

certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).

CLAUSE 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of _____ (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: **INTO University Partnerships Limited**


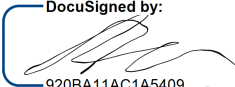
Address: **One Gloucester Place, Brighton, BN1 4AA, United Kingdom**

Contact person's name, position and contact details: John Sykes

Data Protection Officer: Veronica Morrison - privacy@intoglobal.com

Activities relevant to the data transferred under these Clauses:

The recruitment of students, including the Students, to the Programmes or direct enrolment at INTO Partner Universities, and in connection with, and as is necessary for the performance of, each Party's obligations under the Approved International Student Recruitment Counsellor Agreement between INTO and the Counsellor.

Signature  

Date: **Effective from the first date the Counsellor provides Personal Data to INTO**

Role: **Controller**

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

2. Name: **The Counsellor as set out in the Approved International Student Recruitment Counsellor Agreement**

Address: **As set out in the Approved International Student Recruitment Counsellor Agreement**

Contact person's name, position and contact details: **As set out in the Approved International Student Recruitment Counsellor Agreement**

Activities relevant to the data transferred under these Clauses:

The recruitment of students, including the Students, to the Programmes or direct enrolment at INTO Partner Universities, and in connection with, and as is necessary for the performance of, each Party's obligations under the Approved International Student Recruitment Counsellor Agreement between INTO and the Counsellor.

Signature: **The Party's signature of the Counsellor Agreement shall be considered as a signature to these Controller to Controller standard contractual clauses for Personal Data transfers.**

Date: **Effective from the first date the Counsellor provides Personal Data to INTO**

Role: **Controller**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Students for (potential) enrolment with the relevant INTO JV, the relevant INTO Subsidiary or (potential) enrolment on a Direct Entry Programme at an INTO Partner University (as defined in the Counsellor Agreement).

Categories of personal data transferred:

Name, address, date of birth, gender, nationality, email address, phone number, education history and qualification details, GPA, personal statement, photograph, copy of passport, references, portfolio, EU ID card, course information, parental consent (if Student is under 18), visa information and emergency contact details (including name, relationship to data subject and contact number), financial information and information relating to race and ethnic origin, religious beliefs, health, medical and disabilities.

Sensitive data transferred (if applicable):

Applied restrictions and safeguards must fully take into consideration the nature of the data and the risks involved, such as: a strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer:

The Personal Data may be transferred on a continuous basis between the Parties.

Nature of the processing:

The Parties will comply with the additional requirements for Processing the Personal Data as provided in the Counsellor Agreement between the Parties.

Purpose(s) of the data transfer and further processing:

The recruitment of Students to the Programmes, including Direct Entry Programmes, and in connection with, and as is necessary for the performance of, each Party's obligations under the Counsellor Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The Parties will comply with the additional requirements for Processing the Personal Data as provided in the Counsellor Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: ...

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

The Counsellor as the Data Importer shall ensure an appropriate level of security by implementing appropriate technical and organisational measures and shall control compliance with these measures on a regular basis. This includes:

- (a) **Physical access control:** Data Importer shall take reasonable measures to prevent unauthorised persons from gaining access to Personal Data, such as secured buildings, key management and logging of visitors.
- (b) **System access control:** Data Importer shall take reasonable measures to prevent unauthorised access to IT systems such as strong authentication procedures (passwords, double authentication), documented access approvals.
- (c) **Data access control:** Data Importer shall take reasonable measures to prevent unauthorised access to Personal Data such as granting access to personal data granted only on a need-to-know basis, confidentiality obligations and locking of workstations.
- (d) **Data transfer control:** Data Importer shall take reasonable measures to ensure personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); such as data encryption at rest and in transit.
- (e) **Input control:** Data Importer shall take reasonable measures to provide that it is possible retrospectively to check and establish whether and by whom Personal Data has been entered into data processing systems, modified or removed; such as logging systems.
- (f) **Job control:** Data Importer shall take reasonable measures to ensure that Personal Data are processed in accordance with the directions of the Data Exporter such as entering into appropriate data processing agreements with sub-processors.
- (g) **Availability control:** Data Importer shall take reasonable measures to prevent the accidental destruction or loss of the Personal Data.

Official European Commission Footnotes

FN1: Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

FN2: This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

FN3: The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

FN10: That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

FN11: The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

FN12: As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.