# Template H3

# Articulation Agreement

## ARTICULATION AGREEMENT

## BETWEEN

## KINGSTON UNIVERSITY

## AND

## [NAME]

This agreement is made this [DATE]

between

**KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION** whose address is Holmwood House, Grove Crescent, Kingston upon Thames, Surrey KT1 2EE (‘**Kingston**’)

and

# [NAME] whose address is [ADDRESS] (the ‘Institution’)

**Now it is hereby agreed:**

**DEFINITIONS**

**"Applicants"** means individuals on a Named Course at the Institution wishing to come to Kingston to study on a Named Course who pay full Course Fees.

**“Articulation Agreement”** means an agreement whereby Kingston recognises a course of an Institution for prior credit (RPL) for entry to a University Award.

**"Confidential Information"** means information of a confidential nature (including trade secrets and information of commercial value) known to Kingston and concerning Kingston and its products, together with all information provided to the Institution by Kingston in connection with this Agreement and marked "confidential"; completed Application Forms and correspondence with applicants; and any other information, which, if disclosed, may be liable to cause harm to Kingston.

**"Course Fees"** means course fees for the relevant Kingston Named Course, at the time of undertaking the course of study, as amended from time to time by Kingston and publicised on the internet web site [www.kingston.ac.uk](http://www.kingston.ac.uk)

**“Force Majeure”** means any cause preventing either party from performing any or all of its obligations which arises from or is attributable to acts, events, omissions or accidents beyond the reasonable control of the party so prevented including, without limitation, strikes, lockouts or other industrial disputes (whether involving the workforce of the party so prevented or any other party) act of God, war, an act of terrorism, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, or storm, epidemic or pandemic.

**"Named Course(s)"** means any of the taught programmes listed in Schedule 1.

**"UCAS"** means the Universities and Colleges Admissions Service which runs a recruiting service for students in the UK

# Purpose and Form of Collaboration

1.1 This Agreement relates to the transfer of students from the Institution from a Named Course(s) to a Named Course at Kingston. Kingston agrees to recognise and grant automatic entry to applicants from the Institution to enter a programme of study at Kingston at a specified level, provided those applicants meet the requirements set out in this Agreement.

1.2 The Table in Schedule 1 identifies the agreed routes from the Institution’s Named Courses to the relevant Kingston Named Courses. Further course arrangements may be proposed and mutually agreed in future and will be incorporated in a supplement to this Agreement.

1.3 Schedule 2 outlines the quality assurance arrangements that should be put in place to assure the ongoing quality of the Articulation Agreement.

1. **Approval of Agreement**

2.1 As part of its quality assurance role the University will evaluate and determine the quality and ability of the Institution to deliver and assess the prior programme to assure ongoing credit. This is an “approvals event”. The University will require the Agreement to be formally considered at an Approval Panel convened by the University’s Education Committee, which will include the input of an external subject expert. **The University’s regulations state that the commencement of an institutional contract (such as this Agreement) is effective only when the conditions of approval are met.**

2.2 The cost of the approvals event is borne by the Institution. The University will provide the outcomes of the approval, by means of minutes of the committee, to the Institution. The conditions of approval must be met before the University agrees to provide the services and support set out in this Agreement.

2.3 The approvals event shall be in the sole discretion of the University and shall not be subject to the provisions of clauses 11 and 14 of this Agreement as to termination or mediation.

1. **Acceptance of Applicants**

3.1 In all cases acceptance of individual Applicants to the Named Course(s) at Kingston will be based upon:

1. successful completion of and graduation from the Institution’s Named Course
2. attainment of satisfactory level of achievement in English Language;
3. evidence of sufficient financial resources on the part of the Applicant, or their sponsor, to cover the tuition fees and related living costs for the period to be spent at Kingston.
4. the total number of Applicants being no greater than [X]; and
5. written confirmation from the Institution as to i) and ii) above.
6. **Notification of Change in Curriculum**
   1. This Agreement is based upon the curriculum of the Institution and of Kingston at the date of signing.
   2. Any changes made to the Institution’s curriculum will be notified to Kingston by the Institution within a reasonable time and in any event no later than 30 days after such changes have been approved by the Institution.
7. **Process of Application**

5.1 Applications will not be considered on an individual basis as satisfactory completion of the prerequisites outlined in Schedule 1 will guarantee entry to Applicants from the Institution.

5.2 Undergraduate Applicants are, however, required to complete a UCAS application form ([www.ucas.com](http://www.ucas.com)) prior to enrolment at the University. Postgraduate Applicants are required to apply directly to Kingston (details available on [www.kingston.ac.uk](http://www.kingston.ac.uk)).

5.3 Kingston retains the right to verify any Applicant’s identification and to request additional information from the Institution about any Applicant where appropriate.

# Institution’s Duties

The Institution will:

* 1. promote and publicise the Agreement and the opportunity it offers to its

students; and

6.2 identify an office and/or member of staff at the Institution where students interested in continuing their studies at Kingston can find information and advice on how to do so; and

6.3 appoint a member of staff to act as the academic point of contact for each subject area between the two Parties; and

6.4 ensure that the level of English of Applicants meets the level required by Kingston; and

6.5 provide a main point of contact for Kingston at the Institution being [NAME in the Administrative Office].

1. **Kingston’s Duties**

Kingston will:

7.1 provide prospectuses, information, publicity, and other materials to support the Institution in promoting and publicising the programme; and

7.2 appoint a member of staff to act as the academic point of contact for each subject area between the two Parties; and

7.3 establish an efficient process for the admission of Applicants to Kingston; and

7.4 provide a main point of contact for the Institution at Kingston being [NAME in the Faculty].

# Financial arrangements

* 1. In general terms, the costs of activities undertaken by staff of either Party will be borne by the staff member or Party themselves, except where explicitly exempted above.
  2. Successful Applicants will be responsible for their tuition, living, travel and other expenses while studying at Kingston.
  3. Any financial issues not clearly covered by these provisions will be the subject of mutual agreement between the two Parties and will be annexed as a Schedule 3 to this Agreement.

# Duration

* 1. This Agreement will commence on the date above and continue for [X – NB not to exceed 5 years] years from that date.
  2. Renewal of the Agreement will be dependent on a review of the arrangements carried out the year prior to the end of the term of the Agreement, and the signing of a new Agreement.
  3. The duration of this Agreement may be extended by mutual agreement in writing between the Parties.
  4. In any event this Agreement, and any renewals of it under 9.1 & 9.3 above, shall not continue for more than 5 years, without the Articulation process (including due diligence) being completed in full again.

1. **Non-Exclusive Agreement**
   1. This Agreement is not an exclusive agreement. For the avoidance of doubt neither Party shall be prevented from entering into other articulation agreements (or similar) with other Institutions by virtue of entering into this Agreement.

**11. Termination**

11.1 Kingston may terminate this Agreement immediately by giving written notice to the Instituton:

11.1.1 if the Institution is in material breach of this Agreement (and for the avoidance of doubt any breach of confidentiality imposed herein shall be regarded as a material breach for the purposes of this Agreement) and, where the breach is capable of remedy the Institution fails to remedy such breach within thirty days after service of a written notice from Kingston specifying the breach and requiring it to be remedied.

11.1.2 if the Institution should become bankrupt or insolvent, or an administrator or receiver is appointed, or enter into any arrangement with its creditors or take or suffer any similar actions in consequence of a debt or ceases or threatens to cease to carry on business.

11.1.3 if there should be any material change in the management or control of the Institution.

11.1.4 if the Institution engages in any conduct prejudicial to the reputation of Kingston or its marketing generally.

11.1.5 if the Institution purports to assign any or all of this Agreement to a third party without Kingston's consent.

11.2 This Agreement may be terminated by either Party with a minimum of 6 months’ written notice to the other at the address above PROVIDED THAT there is no adverse effect on any Applicants currently studying at Kingston, who should expect to be able to complete their studies once they have commenced.

11.3 The termination of this Agreement howsoever arising is without prejudice to the rights duties and liabilities of either Party accrued prior to termination. The clauses in this Agreement which expressly or impliedly have effect after termination shall continue to be enforceable notwithstanding termination.

11.4 On termination of this Agreement howsoever arising, Kingston will not be liable to pay any sums to the Institution, save that the Institution will be entitled to receive commission, as per clause 7 iii), on current first year Applicants for whom commission remains outstanding, and must destroy or return (as directed by Kingston) all information relating to Kingston within one month of termination.

**12. Tax**

12.1 All sums payable under this Agreement are, unless otherwise stated, inclusive of VAT and other duties or taxes.

12.2 The Institution is responsible for all income tax, National Insurance, VAT or other payments and liabilities connected with any commission paid by Kingston to the Institution.

12.3 Kingston is responsible for all tax or other payments and liabilities connected with any profit made by Kingston from the recruitment of Applicants via the Institution. Each Party is responsible for complying with its local tax regulations relating to this Agreement.

**13. Publicity and Intellectual Property**

13.1 Kingston’s written approval must be obtained before the Institution may use any materials for marketing or publicity in relation to the Named Courses. The Institution will make all stationery, specification sheets or other advertising sales or promotional material, literature or information to be used in connection with the marketing of the Named Courses available for inspection by Kingston.

13.2 The Institution acknowledges that Kingston's rights to any intellectual property used on or in relation to Kingston's business and the goodwill connected with that are Kingston's property and the Institution accepts that it is only permitted to use such intellectual property for the purposes of and during the term of this Agreement and only as authorised by Kingston.

13.3 Except as expressly set out in this Agreement, nothing in this Agreement confers on the Institution any right or interest in any of the trademarks or trade names owned or licensed to Kingston or any right or licence to use or affix any such trademark to any product, nor will the Institution use any trade mark or trade names or get-up which resembles Kingston's trademarks or trading names or logos and which would therefore be likely to confuse or mislead the public or any section of the public.

**14. Anti-Slavery and Human Trafficking**

14.1 The Institution shall reasonably assist Kingston with compliance with the Modern Slavery Act 2015 and shall do nothing which might put Kingston in breach of the Act.

14.2 The Institution shall ensure that slavery and human trafficking is not taking place in any part of its business or in any part of its supply chain.

14.3 The Institution shall implement due diligence procedures for its own suppliers, subcontractors and other participants in its supply chains, to ensure that there is no slavery or human trafficking in its supply chains.

14.4 The Institution hereby warrants that it does not engage in, or condone, the practices of human trafficking, slavery or forced labour in a work environment and that where it has UK workers, those workers are in receipt of the minimum wage.

**15 Anti-corruption, anti-collusion & tax evasion**

15.1 The Institution warrants that it has, will retain in place, and comply with, policies and procedures to avoid the risk of bribery (as set out in the Bribery Act 2010), tax evasion (as set out in the Criminal Finances Act 2017) and fraud within its organisation and in connection with its dealings with other Parties, whether in the UK or overseas.

15.2 The Institution warrants and undertakes that it will not at any time collude with any third party in any way in connection with this Agreement; and, it has not engaged, and will not at any time engage, in any activity, practice or conduct which would constitute tax evasion:

15.4 Any breach of this Clause 15 by the Institution or by anyone employed by it or acting on its behalf shall entitle Kingston to terminate this Agreement forthwith.

**16. Equality and Diversity**

16.1 Each Party shall not, and shall use reasonable endeavours to ensure that, its employees, contractors and agents shall not, harass, victimise or discriminate directly or indirectly against any person on the basis of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation.

**17. General**

17.1 The Institution may not assign, deal with, sub-contract, delegate or dispose of any of its rights under or delegate the burden of this Agreement without the prior written consent of Kingston.

17.2 No failure or delay by any Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

17.3 This Agreement contains all the terms which the parties have agreed in relation to the subject matter of this Agreement and supersedes any prior written or oral agreements, representations or understanding between the Parties relating to such subject matter. Neither Party to this Agreement has been induced to enter into this Agreement by a statement or promise which it does not contain, save that this clause shall not exclude any liability which one Party would otherwise have to the other party in respect of any statement made fraudulently by that Party.

17.4 No variation to this Agreement shall be effective unless in writing signed by or on behalf of both Parties. Any variation will be signed and dated and added to this Agreement as a Schedule.

17.5 Nothing in this Agreement shall constitute or be deemed to constitute a partnership between Kingston and the Institution.

17.6 Should any dispute arise regarding this Agreement, Kingston and the Institution agree to refer the dispute in the first instance to the Vice-Chancellor of Kingston, who will appoint a member of the Senior Leadership Team to make a decision. If that decision is not accepted by either of the Parties the dispute should be referred to mediation, in all but the most exceptional circumstances, before reference is made to arbitration or to the Courts.

17.7 The Institution has no authority to accept fees or any other monies on behalf of Kingston.

17.8 The Institution undertakes to provide Kingston with any reports (public or internal) which describe the quality of the provision in the Institution.

**18. Notices**

18.1 Any notice, demand or communication in connection with this Agreement will be in writing and may be delivered by airmail post or facsimile (but not by e-mail) addressed to the other party at its address at the beginning of this Agreement or its address as the case may be stated below. Notices should be marked for the attention of the Head of International Development for Kingston or [NAME] for the Institution as the case may be (or such address or person as one party shall be notified in writing to the other in accordance with this clause 18.

18.2 The notice, demand or communication will be deemed sufficiently given if it is

provided that the same has been duly committed to the post in a properly addressed and prepaid envelope and will be deemed to have been duly served 14 days after being posted or if delivered by facsimile, at the time of transmission, provided that a confirming copy is sent by airmail post to the other Party within 24 hours after transmission.

18.3 The addresses for the parties are as follows:

In the case of Kingston to: In the case of the Institution to:

Kingston University

Holmwood House [add contact details]

Grove Crescent

Kingston-upon-Thames

KT1 2EE

United Kingdom

Attention: [Name]

Tel Number: +44 (0)20 8417 XXXX

Fax Number: +44 (0)20 8417 XXXX

Email: XXXXX

**19. Rights of Third Parties**

19.1 The Parties to this Agreement do not intend that any of its terms will be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any person not a party to it.

**20. Force Majeure**

20.1 Neither Party to this Agreement shall be deemed to be in breach of this Agreement or otherwise liable to the other Party in any manner whatsoever for any failure or delay in performing its obligations under this Agreement due to Force Majeure.

20.2 If either Party is affected by Force Majeure it shall promptly notify the other Party of the nature and extent of the circumstances in question.

20.3 If the Force Majeure in question continues for more than three months, the Party not subject to the Force Majeure may give notice in writing to the other to terminate this Agreement. The notice to terminate must specify the termination date, which must not be less than fifteen days after the date on which the notice is given, and once such notice has been validly given, this Agreement will terminate on that termination date.

**21. Confidentiality**

21.1 The Institution will keep confidential:

21.1.1 the terms of this Agreement; and

21.1.2 any other Confidential Information that it may acquire in relation to Kingston and/or to this Agreement.

21.2 The Institution will not use Confidential Information for any purpose other than to perform its obligations under this Agreement and will not without the prior written consent of Kingston disclose to any third party any Confidential Information. The Institution will ensure that its officers and employees comply with the provisions of this clause 17.

21.3 The obligations on the Institution set out in clause 17 will not apply to any information which:

21.3.1 is publicly available or becomes available through no act or omission of the Institution; or

21.3.2 the Institution is required to disclose by law or by order of a court of competent jurisdiction.

**22 Freedom of Information**

22.1 Each Party acknowledges that the other Party is or may be subject to the requirements of the Freedom of Information Act 2000 (FOIA), and each Party shall, on request, provide assistance and co-operation to the other as may reasonably request to enable compliance with those requirements.

22.2 Each Party acknowledges that if it is in receipt of a request for information it A may be required under the FOIA to disclose information (including confidential information) without consulting or obtaining consent from the other Party. Each Party shall take reasonable steps to notify the other of receiving a request where reasonably practical for it to do so. The receiving Party shall be responsible for determining in its absolute discretion whether any confidential information and/or any other information is exempt from disclosure in accordance with the FOIA.

**23. Data Protection**

Each Party agrees to comply with its obligations as set out in Schedule 3 (Data Protection) [Select from either schedule 3a, 3b, 3c or 3d as appropriate].

**24. Law and Jurisdiction**

24.1 The formation, existence, construction, performance, validity and all aspects whatsoever of this Agreement or of any term of this Agreement shall be governed by English law. The English courts shall have exclusive jurisdiction to settle any disputes which may arise out of or in connection with this Agreement. The parties agree to submit to the exclusive jurisdiction of the English Courts.

|  |  |
| --- | --- |
| For and on behalf of [INSTITUTION NAME]  [NAME]  [POSITION]  Date | For and on behalf of Kingston University  [NAME]  Vice Chancellor  Date |

**Schedule 1**

**The Courses**

1. **Agreed routes covered by this Agreement**
   1. Courses at the Institution that are specifically covered by this Agreement and recognised by Kingston University.
   2. Applicants who have completed these courses at the Institution, and meet the requirements set out in this agreement, will be granted automatic entry to the Kingston courses specified below:

|  |  |
| --- | --- |
| **Course Name at Institution** | **Kingston University Course and Level of entry. Any pre-requisites for entry should also be stated here.** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* 1. The specific details of the Kingston University courses are set out in the Programme Specification as approved at validation.

**Schedule 2**

**Quality Assurance Arrangements**

The following quality assurance arrangements should be put in place to assure the ongoing quality of the Articulation Agreement.

**Schedule 3a**

**Data Protection**

**(Both Parties Controllers no transfers outside the EEA)**

1. **Definitions**

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| "Applicable EU Law" | means any law of the European Union (or the law of one or more of the Member States of the European Union); |
| "Controller", " Processor" “Processing and "Data Subject" | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| "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 (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("DPA") and EC Directive 95/46/EC (the "DP Directive") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time; |
| "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; |
| "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 L 119/1, 4.5.2016; |
| "ICO" | means the UK Information Commissioner's Office, or any successor or replacement body from time to time; |
| "ICO Correspondence" | means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data; |
| "Losses" | means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| "Permitted Purpose" | means the purpose of the Processing as specified in the Data Protection Particulars; |
| "Personal Data" | means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with the Agreement, and for the purposes of the Agreement includes Sensitive Personal Data (as such particularly described in the Data Protection Particulars); |
| "Personal Data Breach" | has the meaning set out in the Data Protection Laws; |
| "Personal Data Breach Particulars" | means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR; |
| "Personnel" | means all persons engaged or employed from time to time by [the Service Provider] in connection with this Agreement, including employees, consultants, contractors and permitted agents; |
| "Restricted Country" | means a country, territory or jurisdiction outside of the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 25(6) of the DP Directive and/ or Article 45(1) of the GDPR (as applicable); |
| "Security Requirements" | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable; |
| "Sensitive Personal Data" | means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR; |
| "Services" | means the services provided under the Agreement |
| "Third Party Request" | means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation. |

1. **Data Protection**
   1. **Nature of the Processing**
      1. The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:
         1. the Parties shall each Process the Personal Data;
         2. each Party shall act as a Controller in respect of the Processing of the Personal Data on its own behalf and in particular each shall be a Controller of the Personal Data acting individually and in common, as follows:
            1. Each Party shall be a Controller where it is Processing Personal Data it has collated for the purpose of the Agreement
         3. Notwithstanding Paragraph 2.1.1.2, if either Party is deemed to be a joint Controller with the other in relation to the Personal Data, the Parties agree that they shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations set out in Paragraph 3.2.4 where Personal Data has been transmitted by it, or while Personal Data is in its possession or control.
   2. The Parties acknowledge and agree that the Data Protection Particulars below is an accurate description of the data processing:

**Data Protection Particulars**

|  |  |
| --- | --- |
| **The subject matter and duration of the Processing** | The parties will Process Personal Data in the context of: |
| **The nature and purpose of the Processing (‘Permitted Purpose’)** | The Processing will be for the purposes of: |
| **The type of Personal Data being Processed**  **Sensitive Personal Data**  Sensitive personal data includes information about an individual’s  • Race;  • Ethnic origin;  • Political opinions;  • Religion;  • Philosophical beliefs;  • Trade Union membership;  • Genetic data;  • Biometrics;  • Health;  • Sex life; or  • Sexual orientation. | The personal data may include, but is not limited to:  Please tick the boxes that apply and complete  ☐ Personal data – List the type of data below    ☐ Sensitive Personal data – List the type of data below    ☐ Information about criminal records  ☐ Children’s data |
| **The categories of Data Subjects** | The categories of data subjects may include, but are not limited to:  Please tick the boxes that apply and complete  ☐ Students  ☐ Staff  ☐ Other – Give more information below |

* 1. Nothing within this Agreement relieves the either Party of its own direct responsibilities and liabilities under the Data Protection Laws.

1. **Data Controller Obligations**
   1. Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.
   2. Without limiting the generality of the obligation set out in Paragraph 3.1, in particular, each Party shall:
      1. where required to do so make due notification to the ICO;
      2. ensure it is not subject to any prohibition or restriction which would:
         * 1. prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
           2. prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or
           3. prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
      3. ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Personal Data as required in order to obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws;
      4. ensure that appropriate technical and organisational security measures are in place sufficient to comply with the Security Requirements and where requested provide evidence of its compliance promptly.
      5. notify the other Party promptly, and in any event within forty-eight (48) hours of receipt of any Data Subject Request or ICO Correspondence which relates directly or indirectly to the Processing of Personal Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Data Subject Request or ICO Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 3.2.5, each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Data Subject Request or ICO Correspondence;
      6. use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Personal Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
      7. notify the other Party in writing without undue delay of it becoming aware of any actual or suspected Personal Data Breach in relation to the Personal Data received from the other Party and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):

i) implement any measures necessary to restore the security of compromised Personal Data; and

ii) support the other Party to make any required notifications to the ICO and/or other equivalent relevant Regulator and affected Data Subjects;

* + 1. take reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data;
    2. not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
    3. not transfer any Personal Data it is processing to a Restricted Country;
    4. hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data;
    5. at the other Party's option or direction, arrange for the prompt and safe return and/or secure permanent destruction (in accordance with Good Industry Practice) of all Personal Data, together with all copies in its possession or control within 30 days and, where requested by the other Party certify that such destruction has taken place.

1. **Indemnity**
   1. Both Parties shall indemnify on demand and keep indemnified the other Party from and against all and any Losses that are sustained, suffered or incurred by, awarded against or agreed to be paid by the other Party to the extent arising from the first Party's breach of its obligations under this Addendum and/or failure to comply with the Data Protection Laws, including, in particular all Losses resulting from:
      1. any monetary penalties or fines levied by the ICO on the other Party;
      2. the costs of an investigative, corrective or compensatory action required by the ICO, or the defence of a proposed or actual enforcement taken by the ICO;
      3. any Losses suffered or incurred by, awarded against, or agreed to be paid by the other Party pursuant to a claim, action or challenge made by a third party to or against the other Party (including by a Data Subject); and
      4. except to the extent covered by Paragraphs 4.1.10 to 4.1.12, any Losses suffered or incurred, awarded against or agreed to be paid by the other Party.
   2. Nothing in this Agreement shall exclude or limit a Party's liability under this Paragraph 4.

**Schedule 3b**

**Data Protection**

**(University as Controller and Institution as Processor No international transfers outside the EEA)**

1. **Definitions**

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| "Applicable EU Law" | means any law of the European Union (or the law of one or more of the Member States of the European Union); |
| "Controller", " Processor" “Processing” and "Data Subject" | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| "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 (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("DPA") and EC Directive 95/46/EC (the "DP Directive") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time; |
| "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; |
| "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 L 119/1, 4.5.2016; |
| "ICO" | means the UK Information Commissioner's Office, or any successor or replacement body from time to time; |
| "ICO Correspondence" | means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data; |
| "Losses" | means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| "Permitted Purpose" | means the purpose of the Processing as specified in the Data Protection Particulars; |
| "Personal Data" | means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with the Agreement, and for the purposes of the Agreement includes Sensitive Personal Data (as such particularly described in the Data Protection Particulars); |
| "Personal Data Breach" | has the meaning set out in the Data Protection Laws; |
| "Personal Data Breach Particulars" | means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR; |
| "Personnel" | means all persons engaged or employed from time to time by [the Service Provider] in connection with this Agreement, including employees, consultants, Associates and permitted agents; |
| "Restricted Country" | means a country, territory or jurisdiction outside of the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 25(6) of the DP Directive and/ or Article 45(1) of the GDPR (as applicable); |
| "Security Requirements" | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable; |
| "Sensitive Personal Data" | means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR; |
| "Services" | means the services provided under the Agreement |
| "Third Party Request" | means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation. |

1. **General**
   1. Both Parties warrant they will comply with their respective obligations under the Data Protection Laws and this Agreement.
   2. The Parties shall each Process the Personal Data. The Parties acknowledge that the factual arrangements between them dictate the classification of each Party in respect of the Data Protection Laws. The Parties anticipate that the University is the Controller and the Institution is the Processor under this Agreement for the purpose of processing the following Data Protection Particulars:

**Data Protection Particulars**

|  |  |
| --- | --- |
| The subject matter and duration of the Processing | The parties will Process Personal Data in the context of: |
| The nature and purpose of the Processing (‘Permitted Purpose’) | The Processing will be for the purposes of: |
| The type of Personal Data being Processed  Sensitive Personal Data  Sensitive personal data includes information about an individual’s  • Race;  • Ethnic origin;  • Political opinions;  • Religion;  • Philosophical beliefs;  • Trade Union membership;  • Genetic data;  • Biometrics;  • Health;  • Sex life; or  • Sexual orientation. | The personal data may include, but is not limited to:  Please tick the boxes that apply and complete  ☐ Personal data – List the type of data below    ☐ Sensitive Personal data – List the type of data below    ☐ Information about criminal records  ☐ Children’s data |
| The categories of Data Subjects | The categories of data subjects may include, but are not limited to:  Please tick the boxes that apply and complete  ☐ Students  ☐ Staff  ☐ Other – Give more information below |

* 1. Nothing within this Agreement relieves the Institution of its own direct responsibilities and liabilities under the Data Protection Laws.
  2. Each Party shall make due notification to any relevant Regulator.
  3. The Institution undertakes to the University that it will take all necessary steps to ensure that it operates at all times in accordance with the requirements of the Data Protection Laws and will at its own expense assist the University in discharging it obligations under the Data Protection Laws. The Institution shall not, whether by act or omission, cause the University to breach any of its obligations under the Data Protection Laws.

1. **Institution Obligations**

To the extent that the Institution Processes any Personal Data on behalf of the University it shall:

* 1. only Process the Personal Data for and on behalf of the University for the purposes of performing its obligations under the Agreement, and only in accordance with the terms of this Agreement and any documented instructions from the University;
  2. keep a record of any Processing of the Personal Data it carries out on behalf of the University;
  3. unless prohibited by law, notify the University immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable EU Law to act other than in accordance with the instructions of the University, including where it believes that any of the University’s instructions infringe any of the Data Protection Laws;
  4. take, implement and maintain appropriate technical and Organisational security measures which are sufficient to comply with at least the obligations imposed on the University by the Security Requirements and where requested provide to the University evidence of its compliance promptly and in any event within 48 hours.
  5. within thirty (30) calendar days of a request from the University, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the University (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Agreement and provide reasonable information, assistance and co-operation to the University, including access to relevant Personnel and/ or, on the request provide written evidence of its compliance.
  6. not disclose Personal Data to a third party (including a sub-Contractor) in any circumstances without the University's prior written consent, save in relation to Third Party Requests where the Institution is prohibited by law or regulation from notifying the University, in which case it shall use reasonable endeavours to advise the University in advance of such disclosure and in any event as soon as practicable thereafter;
  7. promptly comply with any request from the University to amend, transfer or delete any Personal Data;
  8. notify the University promptly (and in any event with 48 hours) following its receipt of any Data Subject Request or ICO correspondence and shall:
     1. not disclose any Personal Data in response without first consulting with and obtaining the University’s prior written consent; and
     2. provide the University will all reasonable co-operation and assistance in relation to any such Data Subject Request or ICO Correspondence.
  9. notify the University promptly (and in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected, threatened or ‘near miss Personal Data Breach in relation to the Personal Data (and follow-up in writing) and shall:
     1. conduct or support the University in conducting such investigations and analysis that it reasonably requires in respect of such Personal Data Breach;
     2. implement any actions or remedial measures necessary to restore the security of compromised Personal Data; and
     3. assist the University to make any notifications to the ICO and affected Data Subjects;
  10. Comply with the obligations imposed upon a Processor under the Data Protection Laws;
  11. use all reasonable endeavours to assist the University to comply with the obligations imposed on it by the Data Protection Laws, including:
      1. compliance with the Security Requirements;
      2. obligations relating to notifications required by the Data Protection Laws to the ICO and/ or any relevant Data Subjects;
      3. undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the ICO and/or any other relevant Regulator in respect of any such Data Protection Impact Assessments); and
      4. without undue delay and where feasible not later than 72 hours after having become aware of it notify Personal Data Breaches to the ICO and/or any other relevant Regulator unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;
  12. Upon the earlier of: termination or expiry of the Agreement (as applicable); and the date on which Personal Data is no longer relevant to, or necessary for, the Permitted Purpose, the Institution shall cease Processing all Personal Data and return and/ or permanently and securely destroy so that it is no longer retrievable (as directed in writing by the University) all Personal Data and all copies in its possession or control and, where requested, certify that such destruction has taken place (promptly, and in any event within forty-eight (48) hours of the request except to the extent required by Applicable EU Law to retain the Personal Data
  13. Not make (nor instruct or permit a third party to make) a transfer of any Personal Data to a Restricted Country except with the prior written consent of the University and in accordance with any terms the University may impose on such transfer. This shall be as the University deems necessary to satisfy the requirements to ensure that transfers of Personal Data outside of the EEA have adequate protections in place as set out in the Data Protection Laws.

1. **Institutional Personnel**
   1. The Institution shall take all reasonable steps to ensure the reliability and integrity of any of the Personnel who shall have access to Personal Data (including, without limitation, ensuring such Personnel shall have undergone reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data), and ensure that each member of Personnel shall have entered into appropriate contractually-binding confidentiality undertakings.
2. **Appointing Sub-Contractors**
   1. The Institution shall only be permitted to appoint a sub-Contractor in accordance with the Agreement and this Paragraph 5 and to disclose Personal Data to such sub-Contractor for Processing in accordance with the Institution's obligations under the Agreement provided always that:
      1. the Institution undertakes thorough due diligence on the proposed sub-Contractor, including a risk assessment of the information governance-related practices and processes of the proposed sub-Contractor, which shall be used by the Institution to inform any decision on appointing the proposed sub-Contractor;
      2. the Institution provides the University with full details of the proposed sub-Contractor including the results of the due diligence undertaken in accordance with Paragraph 5.1.1 before its appointment and the University has consented to such appointment in writing;
      3. the sub-Contractor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Agreement;
      4. The sub-Contractor’s right to Process Personal Data terminates automatically on expiry or termination of the Agreement for whatever reason.
   2. Notwithstanding any consent or approval given by the University under Paragraph 5.1, the Institution shall remain primarily liable to the University for the acts, errors and omissions of any sub-Contractor to whom it discloses Personal Data, and shall be responsible to the University for the acts, errors and omissions of such sub-Contractor as if they were the Institution's own acts, errors and omissions to the extent that the Institution would be liable to the University under the Agreement for those acts, errors and omissions.
   3. Notwithstanding anything in this Agreement to the contrary, its provisions shall continue in full force and effect for so long as the Service Provider Processes any Personal Data.
3. **Indemnity**
   1. The Institution shall indemnify on demand and keep indemnified the University from and against
      1. any monetary penalties or fines levied by the ICO and/or any other regulator;
      2. the costs of an investigative, corrective or compensatory action required by the ICO or any other regulator or of defending proposed or actual enforcement taken by the ICO or any other regulator;
      3. any losses suffered or incurred by, awarded against, or agreed to be paid by the University pursuant to a claim, action or challenge made by a third party against the University (including by a Data subject);
      4. except to the extent that paragraphs 6.1.1 6.1.2 and/or 6.1.3 apply, any Losses suffered or incurred, awarded against, or agreed to be paid by the University.

in each case to the extent arising as a result of a breach by the Institution (or its sub-Contractors) of this Agreement and/ or their respective obligations under the Data Protection Laws.

6.2 Nothing in this Agreement will exclude limit or restrict the Institution’s liability under the indemnity set out in paragraph 6.1.

1. **Insurance**
   1. The Institution agrees to obtain and keep in full force and effect at all times a policy or policies of insurance which must cover liability for damage arising to any person; apply in relation to the Processing of Personal Data; and have policy limits and provisions conforming to such requirements as the University may from time to time reasonably prescribe;
   2. The Institution shall deliver to the University copies of all applicable insurance policies on demand together with evidence of premiums paid in relation to such insurance.

**Schedule 3c**

**Data Protection**

**(Both Parties Controllers and Institution is outside the EEA)**

1. **Definitions**

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| "Applicable EU Law" | means any law of the European Union (or the law of one or more of the Member States of the European Union); |
| "Controller", " Processor" “Processing and "Data Subject" | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| "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 (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("DPA") and EC Directive 95/46/EC (the "DP Directive") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time; |
| "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; |
| "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 L 119/1, 4.5.2016; |
| "ICO" | means the UK Information Commissioner's Office, or any successor or replacement body from time to time; |
| "ICO Correspondence" | means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data; |
| "Losses" | means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| "Permitted Purpose" | means the purpose of the Processing as specified in the Data Protection Particulars; |
| "Personal Data" | means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with the Agreement, and for the purposes of the Agreement includes Sensitive Personal Data (as such particularly described in the Data Protection Particulars); |
| "Personal Data Breach" | has the meaning set out in the Data Protection Laws; |
| "Personal Data Breach Particulars" | means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR; |
| "Personnel" | means all persons engaged or employed from time to time by [the Service Provider] in connection with this Agreement, including employees, consultants, contractors and permitted agents; |
| "Restricted Country" | means a country, territory or jurisdiction outside of the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 25(6) of the DP Directive and/ or Article 45(1) of the GDPR (as applicable); |
| "Security Requirements" | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable; |
| "Sensitive Personal Data" | means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR; |
| "Services" | means the services provided under the Agreement |
| “Standard Contractual Clauses” | means the Standard Contractual Clauses approved by the European Commission for transfers from Controllers in the European Economic Area to Controllers outside the European Economic Area as updated and/or amended from time to time in their current form attached as Appendix 1 (Standard Contractual Clauses (controller to controller transfers)) to this Agreement. |
| "Third Party Request" | means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation. |

1. Data Protection
   1. **Nature of the Processing**
      1. The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:
         1. the Parties shall each Process the Personal Data;
         2. each Party shall act as a Controller in respect of the Processing of the Personal Data on its own behalf and in particular each shall be a Controller of the Personal Data acting individually and in common, as follows:
            1. Each Party shall be a Controller where it is Processing Personal Data it has collated for the purpose of the Agreement
         3. Notwithstanding Paragraph 2.1.1.2, if either Party is deemed to be a joint Controller with the other in relation to the Personal Data, the Parties agree that they shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations set out in Paragraph 3.2.4 where Personal Data has been transmitted by it, or while Personal Data is in its possession or control.
   2. The Parties acknowledge and agree that the Data Protection Particulars below is an accurate description of the data processing:

**Data Protection Particulars**

|  |  |
| --- | --- |
| The subject matter and duration of the Processing | The parties will Process Personal Data in the context of: |
| The nature and purpose of the Processing (‘Permitted Purpose’) | The Processing will be for the purposes of: |
| The type of Personal Data being Processed  Sensitive Personal Data  Sensitive personal data includes information about an individual’s  • Race;  • Ethnic origin;  • Political opinions;  • Religion;  • Philosophical beliefs;  • Trade Union membership;  • Genetic data;  • Biometrics;  • Health;  • Sex life; or  • Sexual orientation. | The personal data may include, but is not limited to:  Please tick the boxes that apply and complete  ☐ Personal data – List the type of data below    ☐ Sensitive Personal data – List the type of data below    ☐ Information about criminal records  ☐ Children’s data |
| The categories of Data Subjects | The categories of data subjects may include, but are not limited to:  Please tick the boxes that apply and complete  ☐ Students  ☐ Staff  ☐ Other – Give more information below |

* 1. Nothing within this Agreement relieves the either Party of its own direct responsibilities and liabilities under the Data Protection Laws.

1. **Data Controller Obligations**
   1. Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.
   2. Without limiting the generality of the obligation set out in Paragraph 3.1, in particular, each Party shall:
      1. where required to do so make due notification to the ICO;
      2. ensure it is not subject to any prohibition or restriction which would:
         * 1. prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
           2. prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or
           3. prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
      3. ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Personal Data as required in order to obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws;
      4. ensure that appropriate technical and organisational security measures are in place sufficient to comply with the Security Requirements and were requested provide evidence of its compliance promptly.
      5. notify the other Party promptly, and in any event within forty-eight (48) hours of receipt of any Data Subject Request or ICO Correspondence which relates directly or indirectly to the Processing of Personal Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Data Subject Request or ICO Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Paragraph 3.2.5, each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Data Subject Request or ICO Correspondence;
      6. use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Personal Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
      7. notify the other Party in writing without undue delay of it becoming aware of any actual or suspected Personal Data Breach in relation to the Personal Data received from the other Party and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):
2. implement any measures necessary to restore the security of compromised Personal Data; and
3. support the other Party to make any required notifications to the ICO and/or other equivalent relevant Regulator and affected Data Subjects;
   * 1. take reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data;
     2. not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
     3. not transfer any Personal Data it is processing to a Restricted Country;
     4. hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data;
     5. at the other Party's option or direction, arrange for the prompt and safe return and/or secure permanent destruction (in accordance with Good Industry Practice) of all Personal Data, together with all copies in its possession or control within 30 days and, where requested by the other Party certify that such destruction has taken place.
   1. **Transfers of Personal Data to a Restricted Country**.

Notwithstanding the generality of Paragraph 3.2.10, the Parties acknowledge and agree that to the extent that the University transfers data to the Institution it shall be transferring the Personal Data to a Restricted Country in respect of the transfer the Parties shall enter into the Standard Contractual Clauses as set out at Appendix A (Standard Contractual Clauses (controller to controller transfers)) to this Agreement, on the date of this Agreement, such clauses being incorporated into and forming part of this Agreement.

1. **Indemnity**
   1. Both Parties shall indemnify on demand and keep indemnified the other Party from and against all and any Losses that are sustained, suffered or incurred by, awarded against or agreed to be paid by the other Party to the extent arising from the first Party's breach of its obligations under this Addendum and/or failure to comply with the Data Protection Laws, including, in particular all Losses resulting from:
      1. any monetary penalties or fines levied by the ICO on the other Party;
      2. the costs of an investigative, corrective or compensatory action required by the ICO, or the defence of a proposed or actual enforcement taken by the ICO;
      3. any Losses suffered or incurred by, awarded against, or agreed to be paid by the other Party pursuant to a claim, action or challenge made by a third party to or against the other Party (including by a Data Subject); and
      4. except to the extent covered by Paragraphs 4.1.10 to 4.1.12, any Losses suffered or incurred, awarded against or agreed to be paid by the other Party.
   2. Nothing in this Agreement shall exclude or limit a Party's liability under this Paragraph 4.

**Schedule 3c**

**Appendix 1**

**Commission Decision C(2004)5721**

**Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)**

Data transfer agreement

between

**KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION** (name)

of River House, 53 – 57 High Street, Kingston upon Thames, KT1 1LQ (address and country of establishment)

hereinafter “data exporter”

and

(name)

(address and country of establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

**Definitions**

For the purposes of the clauses:

1. “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);
2. “the data exporter” shall mean the controller who transfers the personal data;
3. “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
4. “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

1. **Obligations of the data exporter**

The data exporter warrants and undertakes that:

1. The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
2. It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
3. It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
4. It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
5. It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.
6. **Obligations of the data importer**

The data importer warrants and undertakes that:

1. It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
2. It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.
3. It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.
4. It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
5. It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
6. At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
7. Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.
8. It will process the personal data, at its option, in accordance with:
9. the data protection laws of the country in which the data exporter is established, or
10. the relevant provisions[[1]](#footnote-2) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[[2]](#footnote-3), or
11. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects:

Initials of data importer: ;

1. It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and
2. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
3. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or
4. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
5. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer
6. **Liability and third party rights**
7. Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.
8. The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).
9. **Law applicable to the clauses**

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

1. **Resolution of disputes with data subjects or the authority**
2. In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
3. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
4. Each party shall abide by a decision of a competent court of the data exporter’s country of establishment or of the authority which is final and against which no further appeal is possible.
5. **Termination**
6. In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.
7. In the event that:
8. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);
9. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
10. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
11. a final decision against which no further appeal is possible of a competent court of the data exporter’s country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
12. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.
13. Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.
14. The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.
15. **Variation of these clauses**

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

1. **Description of the Transfer**

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:

FOR DATA IMPORTER FOR DATA EXPORTER

**Schedule 3c**

**Annex A**

**Data Processing Principles**

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

b) where otherwise provided by the law of the data exporter.

**Schedule 1c**

**Annex B**

**Description of the Transfer**

(To be completed by the parties)

**Data subjects**The personal data transferred concern the following categories of data subjects:  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Purposes of the transfer(s)**  
The transfer is made for the following purposes:  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Categories of data**  
The personal data transferred concern the following categories of data:  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Recipients**  
The personal data transferred may be disclosed only to the following recipients or categories of recipients:  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Sensitive data** (if appropriate)  
The personal data transferred concern the following categories of sensitive data:  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Data protection registration information of data exporter** (where applicable)  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Additional useful information** (storage limits and other relevant information)  
………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**Contact points for data protection enquiries**

**Data importer Data exporter**………………………………………… ………………………………………

………………………………………… ………………………………………

**Schedule 3d**

**Data Protection**

**(University as Controller and Institution as Processor**

**International transfers outside the EEA)**

* 1. **Definitions**

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| **"Applicable EU Law"** | means any law of the European Union (or the law of one or more of the Member States of the European Union); |
| **"Controller" "Processor" “Processing” and "Data Subject"** | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| "**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 (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("**DPA**") and EC Directive 95/46/EC (the "**DP Directive**") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time; |
| "**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; |
| "**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 L 119/1, 4.5.2016; |
| "**ICO**" | means the UK Information Commissioner's Office, or any successor or replacement body from time to time; |
| "**ICO Correspondence**" | means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data; |
| **"Losses"** | means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| "**Permitted** **Purpose**" | means the purpose of the Processing as specified in the Data Protection Particulars; |
| "**Personal Data**" | means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with the Agreement, and for the purposes of the Agreement includes Sensitive Personal Data (as such particularly described in the Data Protection Particulars); |
| "**Personal Data Breach**" | has the meaning set out in the Data Protection Laws; |
| **"Personal Data Breach Particulars"** | means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR; |
| "**Personnel**" | means all persons engaged or employed from time to time by [the Service Provider] in connection with this Agreement, including employees, consultants, contractors and permitted agents; |
| "**Restricted Country**" | means a country, territory or jurisdiction outside of the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 25(6) of the DP Directive and/ or Article 45(1) of the GDPR (as applicable); |
| "**Security Requirements**" | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable; |
| **"Sensitive Personal Data"** | means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR; |
| **"Services"** | means the services provided under the Agreement |
| **“Standard Contractual Clauses”** | means the Standard Contractual Clauses approved by the European Commission for transfers from Controllers in the European Economic Area to Processors outside the European Economic Area as updated and/or amended from time to time and in their current form attached as Appendix 1 (Standard Contractual Clauses (Processors)) to this Agreement |
| "**Third Party Request**" | means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation. |

* 1. **General**
  2. Both Parties warrant they will comply with their respective obligations under the Data Protection Laws and this Agreement.
  3. The Parties shall each Process the Personal Data. The Parties acknowledge that the factual arrangements between them dictate the classification of each Party in respect of the Data Protection Laws. The Parties anticipate that the University is the Controller, and the Institution is the Processor under this Agreement for the purpose of processing the following Data Protection Particulars:

**Data Protection Particulars**

|  |  |
| --- | --- |
| **The subject matter and duration of the Processing** | The parties will Process Personal Data in the context of: |
| **The nature and purpose of the Processing (‘Permitted Purpose’)** | The Processing will be for the purposes of: |
| **The type of Personal Data being Processed**  **Sensitive Personal Data**  Sensitive personal data includes information about an individual’s  • Race;  • Ethnic origin;  • Political opinions;  • Religion;  • Philosophical beliefs;  • Trade Union membership;  • Genetic data;  • Biometrics;  • Health;  • Sex life; or  • Sexual orientation. | The personal data may include, but is not limited to:  Please tick the boxes that apply and complete  ☐ Personal data – List the type of data below    ☐ Sensitive Personal data – List the type of data below    ☐ Information about criminal records  ☐ Children’s data |
| **The categories of Data Subjects** | The categories of data subjects may include, but are not limited to:  Please tick the boxes that apply and complete  ☐ Students  ☐ Staff  ☐ Other – Give more information below |

* 1. Nothing within this Agreement relieves the Institution of its own direct responsibilities and liabilities under the Data Protection Laws.
  2. Each Party shall make due notification to any relevant Regulator.
  3. The Institution undertakes to the University that it will take all necessary steps to ensure that it operates at all times in accordance with the requirements of the Data Protection Laws and will at its own expense assist the University in discharging it obligations under the Data Protection Laws. The Institution shall not, whether by act or omission, cause the University to breach any of its obligations under the Data Protection Laws.
  4. **Institutional Obligation**

To the extent that the Institution Processes any Personal Data on behalf of the University it shall:

* 1. only Process the Personal Data for and on behalf of the University for the purposes of performing its obligations under the Agreement, and only in accordance with the terms of this Agreement and any documented instructions from the University;
  2. keep a record of any Processing of the Personal Data it carries out on behalf of the University;
  3. unless prohibited by law, notify the University immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable EU Law to act other than in accordance with the instructions of the University, including where it believes that any of the University’s instructions infringe any of the Data Protection Laws;
  4. take, implement and maintain appropriate technical and organisational security measures which are sufficient to comply with at least the obligations imposed on the University by the Security Requirements and where requested provide to the University evidence of its compliance promptly and in any event within 48 hours.
  5. within thirty (30) calendar days of a request from the University, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the University (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Agreement and provide reasonable information, assistance and co-operation to the University, including access to relevant Personnel and/ or, on the request provide written evidence of its compliance.
  6. not disclose Personal Data to a third party (including a sub-contractor) in any circumstances without the University's prior written consent, save in relation to Third Party Requests where the Institution is prohibited by law or regulation from notifying the University, in which case it shall use reasonable endeavours to advise the University in advance of such disclosure and in any event as soon as practicable thereafter;
  7. promptly comply with any request from the University to amend, transfer or delete any Personal Data;
  8. notify the University promptly (and in any event with 48 hours) following its receipt of any Data Subject Request or ICO correspondence and shall:
     1. not disclose any Personal Data in response without first consulting with and obtaining the University’s prior written consent; and
     2. provide the University will all reasonable co-operation and assistance

in relation to any such Data Subject Request or ICO

Correspondence.

* 1. notify the University promptly (and in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected, threatened or ‘near miss’ Personal Data Breach in relation to the Personal Data (and follow-up in writing) and shall:
     1. conduct or support the University in conducting such investigations and analysis that it reasonably requires in respect of such Personal Data Breach;
     2. implement any actions or remedial measures necessary to restore the security of compromised Personal Data; and
     3. assist the University to make any notifications to the ICO and affected Data Subjects;
  2. Comply with the obligations imposed upon a Processor under the Data Protection Laws;
  3. use all reasonable endeavours to assist the University to comply with the obligations imposed on it by the Data Protection Laws, including:
     1. compliance with the Security Requirements;
     2. obligations relating to notifications required by the Data Protection Laws to the ICO and/ or any relevant Data Subjects;
     3. undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the ICO and/or any other relevant Regulator in respect of any such Data Protection Impact Assessments); and
     4. without undue delay and where feasible not later than 72 hours after having become aware of it notify Personal Data Breaches to the ICO and/or any other relevant Regulator unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.
  4. Upon the earlier of: termination or expiry of the Agreement (as applicable); and the date on which Personal Data is no longer relevant to, or necessary for, the Permitted Purpose, the Institution shall cease Processing all Personal Data and return and/ or permanently and securely destroy so that it is no longer retrievable (as directed in writing by the University) all Personal Data and all copies in its possession or control and, where requested, certify that such destruction has taken place (promptly, and in any event within forty-eight (48) hours of the request except to the extent required by Applicable EU Law to retain the Personal Data
  5. **Transfer of Personal Data to a Restricted Country**

3.13.1 Not make (nor instruct or permit a third party to make) a transfer of any Personal Data to a Restricted Country.

3.13.2 Notwithstanding the generality of Paragraph 3.13.1 the Parties acknowledge and agree that to the extent the University transfers Personal Data to the Institution, it shall be transferring Personal Data to a Restricted Country.

3.13.3 In respect of the transfer in Paragraph 3.13.2 the Parties shall enter into the Standard Contractual Clauses, as set out at Appendix A (Standard Contractual Clauses (Processors)) to this Agreement, on the date of this Agreement, such clauses being incorporated into and forming part of this Agreement.

**4. Institutional Personnel**

4.1 The Institution shall take all reasonable steps to ensure the reliability and integrity of any of the Personnel who shall have access to Personal Data (including, without limitation, ensuring such Personnel shall have undergone reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data), and ensure that each member of Personnel shall have entered into appropriate contractually-binding confidentiality undertakings.

1. **Appointing Sub-Contractors**
   1. The Institution shall only be permitted to appoint a sub-contractor in accordance with the Agreement and this Paragraph 5.1 and to disclose Personal Data to such sub-contractor for Processing in accordance with the Institution's obligations under the Agreement provided always that:
      1. the Institution undertakes thorough due diligence on the proposed sub-contractor, including a risk assessment of the information governance-related practices and processes of the proposed sub-contractor, which shall be used by the Institution to inform any decision on appointing the proposed sub-contractor;
      2. the Institution provides the University with full details of the proposed sub-contractor including the results of the due diligence undertaken in accordance with Paragraph 5.1.1 before its appointment and the University has consented to such appointment in writing;
      3. the sub-contractor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Agreement;
      4. The sub-contractor’s right to Process Personal Data terminates automatically on expiry or termination of the Agreement for whatever reason.
   2. Notwithstanding any consent or approval given by the University under Paragraph 5.1, the Institution shall remain primarily liable to the University for the acts, errors and omissions of any sub-contractor to whom it discloses Personal Data, and shall be responsible to the University for the acts, errors and omissions of such sub-contractor as if they were the Institution's own acts, errors and omissions to the extent that the Institution would be liable to the University under the Agreement for those acts, errors and omissions.
   3. Notwithstanding anything in this Agreement to the contrary, its provisions shall continue in full force and effect for so long as the Service Provider Processes any Personal Data.
2. **Indemnity**
   1. The Institution shall indemnify on demand and keep indemnified the University from and against
      1. any monetary penalties or fines levied by the ICO and/or any other regulator
      2. the costs of an investigative, corrective or compensatory action required by the ICO or any other regulator or of defending proposed or actual enforcement taken by the ICO or any other regulator.
      3. any losses suffered or incurred by, awarded against, or agreed to be paid by the University pursuant to a claim, action or challenge made by a third party against the University (including by a Data subject)
      4. except to the extent that paragraphs 6.1.1 6.1.2 and/or 6.1.3 apply, any Losses suffered or incurred, awarded against, or agreed to be paid by the University in each case to the extent arising as a result of a breach by the Institution (or its sub-contractors) of this Agreement and/ or their respective obligations under the Data Protection Laws.

Nothing in this Agreement will exclude limit or restrict the Institution’s liability under the indemnity set out in paragraph 6.1.

1. **Insurance**
   1. The Institution agrees to obtain and keep in full force and effect at all times a policy or policies of insurance which must cover liability for damage arising to any person; apply in relation to the Processing of Personal Data; and have policy limits and provisions conforming to such requirements as the University may from time to time reasonably prescribe;
   2. The Institution shall deliver to the University copies of all applicable insurance policies on demand together with evidence of premiums paid in relation to such insurance.

**Schedule 3d**

**Appendix A**

**Commission Decision C(2010)593  
Standard Contractual Clauses (Processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:Kingston University Higher Education Corporation

Address: River House, 53 – 57 High Street, Kingston upon Thames, KT1 1LQ

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……………………………………………………………  
(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

…………………………………………………………………  
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

**Definitions**

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[[3]](#footnote-4);

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law****'*** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

**Obligations of the data importer[[4]](#footnote-5)**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

**Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

**Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely……England and Wales

Clause 10

**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

**Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[[5]](#footnote-6). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the United Kingdom

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

**Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1

**On behalf of the data exporter:**

Name (written out in full): ……………………………………………………………………….

Position: ……………………………………………………………………………………………………

Address: ………………………………………………………………………………………………….

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

**On behalf of the data importer:**

Name (written out in full): ……………………………………………………………………….

Position: ……………………………………………………………………………………………………

Address: ………………………………………………………………………………………………….

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

………………………………………………………………………………………………………………………………………………………………………………………………

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

………………………………………………………………………………………………………………………………………………………………………………………………

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER

Name:………………………………

Authorised Signature ……………………

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

1. “Relevant provisions” means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses). [↑](#footnote-ref-2)
2. However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected. [↑](#footnote-ref-3)
3. Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↑](#footnote-ref-4)
4. Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter* *alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-5)
5. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-6)