**Schedule 5d**

1. schedule 5D - DATA PROTECTION
2. University to Controller (no restricted international Transfers)
3. DEFINITIONS

In this Schedule the following definitions shall apply:

|  |  |
| --- | --- |
| "**Applicable Law**" | means all applicable laws, statutes, enactments, regulations, declarations decrees, directives, legislative enactments, orders, binding decisions of a competent Court or Tribunal, regulations, rules, regulatory policies, guidelines, codes, other binding restrictions, regulatory permits and licences applicable under law which are in force from time to time during the term of the Agreement, including the rules, codes of conduct, codes of practice, practice requirements and accreditation terms stipulated by any regulatory authority or body to which a Party is subject from time to time as the same are amended, consolidated, modified, re-enacted or replaced; |
| **"Controller"** | means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; |
| "**Data Exporter**" | means a Party making or proposing to make a transfer of Personal Data which is a Restricted Transfer; |
| "**Data Importer**" | means a Party in receipt of Personal Data as a result of a Restricted Transfer; |
| "**Data Originator**" | means the Party from whom the Shared Data originates; |
| "**Data Processing Particulars**" | means, in relation to any Processing under this Agreement:  the subject matter and duration of the Processing;  the nature and purpose of the Processing;  the type of Personal Data being Processed; and  the categories of Data Subjects;  as set out in Appendix 1; |
| "**Data Protection Impact Assessment"** | means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data which includes as a minimum:  a systematic description of the envisaged Processing and the purposes of the Processing, including, where applicable, the legitimate interest for which the Processing is carried out;  an assessment of the necessity and proportionality of the Processing operations in relation to the purposes pursued;  an assessment of the risks to the rights and freedoms of Data Subjects; and  the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the Data Protection Laws; |
| **"Data Protection Laws"** | means:  any Applicable Law to which a Party is subject from time to time in any territory in which they Process Personal Data and which relates to the protection of individuals with regards to the Processing of Personal Data and privacy rights, including without limitation the GDPR (General Data Protection) and the e-Privacy Directive and relevant member state laws in the European Economic Area ("**EEA**") and in relation to the United Kingdom ("**UK**") the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (amended by SI 2011 no. 6) and the GDPR (as incorporated into UK law under the UK European Union (Withdrawal) Act 2018) as the same are amended in accordance with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by SI 2020 no. 1586), as amended to be referred to as **PECR**, **DPA 2018** and the **UK GDPR** respectively, as the same are amended, consolidated, modified, re-enacted or replaced from time to time;  any code of practice or guidance published by a Regulator from time to time; and/or  any binding pronouncements (including findings, orders, decisions and/or judgements) issued by a Regulator or a court; |
| **"Data Subject"** | means an identified or identifiable natural person to whom Personal Data relates, regardless of whether the person can be identified directly or indirectly; |
| **"Data Subject Request"** | * + - 1. means an actual or purported request or notice or complaint from or on behalf of a Data Subject exercising his/her rights under the Data Protection Laws 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"** | * + - 1. 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; |
| "**Group**" | means in respect of either Party, that Party, its holding company, its subsidiaries and any other direct or indirect holding company or subsidiary from time to time of such holding company or subsidiary; |
| **"Joint Controllers"** | means where two or more Controllers jointly determine the purposes and means of processing of Personal Data; |
| **"Losses"** | * + - 1. 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 Recipients"** | * + - 1. means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Appendix 1*;* |
| **"Personal Data"** | means any information relating to a Data Subject, including but not limited to any Special Category Personal Data and data relating to criminal convictions and offences; |
| **"Personal Data Breach"** | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed and, for the avoidance of doubt, includes a breach of Paragraph 2.4.2(h); |
| **"Personnel"** | means all persons engaged or employed from time to time by the Associate in connection with this Agreement, including employees, consultants, contractors and permitted agents from time to time; |
| **"Process"** | means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (and "**Processing**" and "**Processed**" shall be construed accordingly); |
| **"Processor"** | means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller; |
| **"Regulator"** | means any local or national agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering, providing guidance on, supervising and enforcing Data Protection Laws, including in the United Kingdom the Information Commissioner's Office, or any successor or replacement body from time to time; |
| **"Regulator Correspondence"** | means any correspondence or communication (whether written or verbal) from a Regulator in relation to the Processing of Personal Data; |
| **"Restricted Country"** | means a country, territory or jurisdiction which: (i) is not covered by an adequacy determination by a competent authority with jurisdiction over the Data Exporter; (ii) or otherwise in relation to which a transfer restriction applies under the Applicable Laws of the Data Exporter; |
| "**Restricted Transfer**" | means:  a transfer of Shared Data to a Restricted Country; or  an onward transfer from a Data Importer to a third party,  in each case where such transfer would be prohibited by Data Protection Laws of the Data Exporter in the absence of a legal transfer mechanism permitted by the Data Protection Laws; |
| **"Security Requirements"** | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws including, in particular:  a requirement to only Process Personal Data in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;  a requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The appropriate level of security shall be assessed by taking into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed; |
| **"Services"** | means as defined in the main agreement. |
| **"Shared Data"** | means the Personal Data shared between the Parties under, or in connection with, this Agreement (such Personal Data is more particularly described in Appendix 1); |
| "Special Category Personal Data” | means information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation; |
| "**Sub-Processor**" | means any third party Processor appointed by the Associate (including a sub-contractor or any Group company or affiliate, or any Data Importer) to Process the Shared Data on its behalf in connection with the Services (including any sub-Processors of such Sub-Processor) and "**Sub-Processing**" relates to Processing carried out by a Sub-Processor; and |
| "**Third Party Request**" | means a written request from any third party for disclosure of (or access to) Shared Data, including a Data Subject Request (or purported Data Subject Request), a request to rectify, block or erase any Personal Data, any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation, a Government Access request or otherwise, where compliance with such request is required or purported to be required by Applicable Law. |

**DATA PROTECTION**

Arrangement Between the Parties

* + 1. The Parties each acknowledge and agree that the factual arrangements between them dictate the classification and 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:

the Parties shall each Process the Shared Data;

each Party shall act as a Controller in respect of the Processing of the Shared Data on its own behalf and in particular each shall be a Controller of the Shared Data acting individually and in common, as follows:

the University shall be a Controller where it is Processing the Shared Data in relation to Higher Education (to enable the institution to register students at Kingston University and for Kingston University to provide services under the contract, e.g. Award), and

the Associate shall be a Controller where it is Processing the Shared Data in relation to Higher Education (e.g. in order to manage the student relationship with the Associate)**.**

[each Party shall act as a Controller in respect of the Processing of the Shared Data as Joint Controllers in relation to [insert purpose];] ***[Guidance Note: Only include if the parties will act as joint controllers and if so, insert purpose for which they will be processing the Shared Data as joint controllers.]***

* + 1. Notwithstanding Paragraph 2.1.1(b), if either Party is deemed to be a Joint Controller with the other in relation to the Shared 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 2.4.2(h) where Shared Data has been transmitted by it, or while Shared Data is in its possession or control; and

acting reasonably and in good faith seek by way of variation or additional agreement or arrangement, to document the parties' respective obligations in accordance with Data Protection Laws (particularly in respect of communications with Data Subjects, third parties and a Regulator, including in respect of transparency requirements and notification obligations).

* 1. Each of the Parties acknowledges and agrees that Appendix 1 to this Agreement is an accurate description of the Data Processing Particulars.

Contact Data

* + 1. Notwithstanding Paragraph 2.1 the Parties each acknowledge and agree that they may need to Process Personal Data in relation to each Party's representatives (in their respective capacities as Controllers) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Agreement and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Services; and (f) comply with their respective regulatory obligations.
    2. Each Party shall Process such Personal Data for the purposes set out in Paragraph 2.3.1 in accordance with their respective privacy policies. The Parties acknowledge that they may be required to share Personal Data with members of their Group and other relevant parties, within or outside of the country of origin, in order to carry out the activities listed in Paragraph 2.3.1, and in doing so each Party will ensure that the sharing and use of this Personal Data complies with applicable Data Protection Laws.

Data Controller Obligations

* + 1. Each Party shall in relation to the Processing of the Shared Data comply at all times with its respective obligations under the Data Protection Laws.
    2. Without limiting the generality of the obligation set out in Paragraph 2.4.1, in particular, each Party shall:
       1. only Process the Shared Data for the purposes of providing the Services or taking the benefit of the Services (as applicable) or otherwise in accordance with the terms of this Agreement
       2. where required to do so make due notification and make all payments due (as applicable) to the Regulator;
       3. ensure it is not subject to any prohibition or restriction which would:

prevent or restrict it from disclosing or transferring the Shared Data to the other Party as required under this Agreement;

prevent or restrict it from granting the other Party access to the Shared Data as required under this Agreement; or

prevent or restrict either Party from Processing the Shared Data, as envisaged under this Agreement;

* + - 1. 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 Shared 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.
      2. maintain complete and accurate records and information to demonstrate its compliance with this Paragraph 2.4 (Data Controller Obligations);
      3. work together (acting reasonably and in good faith) in the preparation of any Data Protection Impact Assessment (where applicable) prior to commencing any Processing and continue to review the requirement for any Data Protection Impact Assessments should there be a change in the intended purpose for the Processing of the Personal Data;
      4. ensure that the Shared Data disclosed or transferred to, or accessed by, the other Party is accurate and up-to-date, as well as adequate, relevant and not excessive to enable the other Party to Process such Shared Data as envisaged under this Agreement;
      5. ensure that appropriate technical and organisational security measures are in place sufficient to comply with at least the obligations imposed on the Controller by the Security Requirements and at any time where requested provide to the other Party evidence of its compliance.
      6. notify the other Party promptly, and in any event within 24 hours of receipt of any Third Party Requestor Regulator Correspondence which relates directly or indirectly to the Processing of the Shared Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Third Party Request or Regulator 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 2.4.2(i), each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Third Party Request or Regulator Correspondence. [Where acting as a Joint Controller, the Party who has provided the notice (and/or as applicable obtained the necessary consent(s)) pursuant to Paragraph 2.4.2(d) shall be responsible for responding to a Third Party Request or Regulator correspondence and the other Party shall provide all such reasonable assistance as may be required];
      7. use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Shared Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
      8. notify the other Party in writing without undue delay (and in any event within 24 hours upon becoming aware of any actual or suspected or threatened Personal Data Breach in relation to the Shared Data ("Data Loss Event") and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):
         1. seek to recover the compromised data as soon as practicable and implement any measures necessary to restore the security of the compromised Shared Data;
         2. promptly provide the other Party with a report containing details about the nature of the Data Loss Event and provide the other Party with further information in phases, as details become available;
         3. investigate the incident and its cause;
         4. support the other Party to make any required notifications to the Regulator and/or other relevant regulatory body and affected Data Subjects. [Where acting as a Joint Controller;

the Party who has suffered the actual or suspected Data Loss Event shall be responsible (with the support of the other joint Controller(s)) for making any required notification to a Regulator; and

the Party who has provided the notice (and/or as applicable obtained the necessary consent(s)) pursuant to Paragraph 2.4.2(d) shall be responsible (with the support of the other joint Controller(s)) for making any required notification to affected Data Subjects; and

* + - * 1. co-ordinate with the other Party the management of public relations and public statements relating to the incident. For the avoidance of doubt the Associate shall make no public statement in relation to the incident without the prior written approval of the University.
      1. take reasonable steps to ensure the reliability of and adequate training of any of its Personnel who have access to the Shared 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 Shared Data it is processing to a Restricted Country except in accordance with Paragraph 3;
      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. [except to the extent required by Applicable Law, upon the earlier of:
         1. termination or expiry of this Agreement; and/ or
         2. the date on which the Shared Data is no longer relevant to, or necessary for, the provision of the Services,

cease Processing all Shared Data received from the Data Originator and return and/ or permanently and securely destroy such Shared Data and all copies in its possession or control (such that the Shared Data is no longer retrievable), as directed in writing by the Data Originator.

* 1. Each Party will transfer Shared Data to the other in a format agreed between the Parties, which shall apply to each and every occasion that Shared Data is transferred between the Parties, unless agreed otherwise between the Parties.
  2. Where acting as a Controller or Joint Controller, before further sharing the Shared Data with a:
     1. third party where such party shall act as a Controller, the Associate must obtain the consent of the University and enter into an appropriate data sharing agreement with the third party and ensure such third party meets the requirements of the Data Protection Laws and only uses the Shared Data for the purposes permitted and set out in this Agreement.
  3. Except as otherwise provided, this Agreement does not transfer ownership of, or create any licences (implied or otherwise), in any intellectual property rights in any Personal Data.

INTERNATIONAL TRANSFERS

* 1. The Associate shall not make a Restricted Transfer without the prior written consent of the University and without taking such measures as are necessary to ensure the transfer is in compliance with Data Protection Laws.

**Recoverable Loss AND COMPENSATION**

* 1. Nothing in this Agreement shall prevent the University from recovering any Losses it incurs in relation to:
     1. legal fees, on a solicitor/client basis;
     2. other professional charges and expenses;
     3. disbursements;
     4. costs of investigation including forensic investigation;
     5. cost of breach notification, including notifications to Data Subjects, Regulator(s) or any other parties including listing authorities whether notification is required under Applicable Law or otherwise made in the reasonable belief that notification is necessary;
     6. cost of complaints handling, including providing Data Subjects with credit and/or fraud monitoring services and/or credit reference checks, setting up contact centres (e.g. call centres), and making ex gratia payments;
     7. costs of claims;
     8. cost of litigation;
     9. costs of settlement, including ex gratia payments;
     10. judgment interest; and
     11. penalties, including fines.
  2. To the extent that the Associate has an entitlement under Data Protection Laws to claim from the University compensation paid by the Associate to a Data Subject or third party as a result of a breach of Data Protection Laws (in full or in part) by the University, the University shall be liable only for such amount as directly relates to the University’s responsibility for any damage caused to the relevant Data Subject or third party. For the avoidance of doubt the University shall only be liable to make payment to the Associate under this Paragraph 5.2, upon receipt of evidence from the Associate, which shall be to the University’s reasonable satisfaction and that clearly demonstrates:
     1. that the University has breached Data Protection Laws;
     2. that such breach contributed (in part or in full) to the harm caused entitling the relevant Data Subject or third party to receive compensation in accordance with Data Protection Laws; and
  3. the proportion of responsibility for the harm caused to the relevant Data Subject or third party which is attributable to the University.

INDEMNITY

* 1. Both Parties shall indemnify on demand and keep indemnified and held harmless 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 Schedule **5d** (Data Protection) 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 any Regulator on the other Party;
     2. the costs of any investigative, corrective or compensatory action required by a Regulator, or of defending any proposed or actual enforcement taken by a Regulator including if such investigation arises as a result of a self-report or otherwise;
     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 (or on behalf of) a Data Subject); and
     4. except to the extent covered by Paragraphs 6.1.1 and/ or 6.1.2 and/ or 6.1.3, any Losses suffered or incurred, awarded against or agreed to be paid by the other Party.]

INSURANCE

* 1. Both Parties agree:
     1. to obtain and keep in full force and effect at all times, in respect of the Processing of the Personal Data, a policy or policies of insurance covering liability for damage arising to persons as a result of the Party's breach of this Schedule **5d** (Data Protection) and/or failure to comply with the Data Protection Laws and which meet the following conditions:
        1. it must cover liability for damage arising to any person;
        2. it must apply in relation to the Processing of Personal Data;

**AUDIT**

The Associate shall within 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 Schedule.

**termination**

* 1. Notwithstanding anything in this Agreement to the contrary, this Schedule shall continue in full force and effect for so long as either Party Processes any Shared Data received from the other Party.
  2. In the case of any non-compliance by the Associate with any of the obligations under this Agreement, the Data Protection Laws, the University may, by giving written notice unilaterally:
     1. immediately terminate this Agreement; and/or
     2. suspend any data submission under this Agreement; and/or
     3. require the Associate to cease or suspend any Processing of Shared Data including in specific locations or by specific Sub-Processors.

GOVERNING LAW

This Schedule **5d** shall be governed by and construed in accordance with English Law.

Appendix 1

Data Protection Particulars

|  |  |
| --- | --- |
| **The subject matter and duration of the Processing** | The subject matter as defined in the Agreement for the duration of the Agreement |
| **The nature and purpose of the Processing** | Higher Education to enable the institution to register students at Kingston University and for Kingston University to provide services under the contract, e.g. Award. |
| **The type of Personal Data being Processed** | Highlight relevant Personal Data:  Name  Date of birth  Address  Nationality  Next of kin  Student records  Staff info relevant to service delivery  Other: Other information the parties are required to hold as part of their statutory reporting duties.  Highlight relevant Special Category Personal Data/criminal convictions:  Race or ethnic origin  Physical or mental health  Criminal convictions and offences |
| **The categories of Data Subjects** | Highlight categories below:  Students  Staff  Other N/A |
| **Data Retention/Deletion Period and Process** | In line with Kingston University Retention Policy. |
| **Locations (including the geographic region) in which the personal data may be Processed by the Associate** | Kingston University, Holmwood House, Grove Crescent, Kingston upon Thames, Surrey, KT1 2EE, United Kingdom  [insert Associate name and location] |

Page 23 of 23