

Memorandum of Cooperation  
Appendix: 5  
Data Processing Agreement

1. DEFINITIONS

In this agreement, the following definitions shall apply:

<b>"College"</b>	means Royal Holloway, University of London;
<b>"Controller", "Processor" "Data Subject" and "Data Protection Officer"</b>	shall have the meaning given to those terms in the applicable Data Protection Laws;
<b>"Data Protection Laws"</b>	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 (" <b>DPA</b> ") and EC Directive 95/46/EC (the " <b>DP Directive</b> ") (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; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;
<b>"Data Processing Particulars"</b>	means, in relation to any Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects; as set out in section 2.2.
<b>"Data Subject Request"</b>	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;
<b>"GDPR"</b>	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;
<b>"ICO"</b>	means the UK Information Commissioner's Office, or any successor or replacement body from time to time;

<b>"ICO Correspondence"</b>	means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data;
<b>Permitted Recipients"</b>	means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Paragraph 2.3
<b>"Personal Data"</b>	means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with this Agreement, and for the purposes of this Agreement includes Sensitive Personal Data (as such Personal Data is more particularly described in Paragraph 2.3 ;
<b>"Personal Data Breach"</b>	has the meaning set out in the Data Protection Laws and for the avoidance of doubt , includes a breach of Paragraph 2.2.2(e);
<b>"Processing"</b>	has the meaning set out in the Data Protection Laws (and <b>"Process"</b> and <b>"Processed"</b> shall be construed accordingly);
<b>"Restricted Country"</b>	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);
<b>"RHSU"</b>	means Royal Holloway Students' Union;
<b>"Security Requirements"</b>	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;
<b>"Sensitive Personal Data"</b>	means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR;
<b>"Services"</b>	means the Services as described in Paragraph 2.3; and
<b>"Third Party Request"</b>	means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation.

## 2. DATA PROTECTION

### 2.1 Nature of the Processing

2.1.1 The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Each Party agrees that the nature of the Processing under this Agreement will be as follows:

- (a) the Parties shall each Process the Personal Data;

- (b) 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:
  - (i) The College shall be a Controller where it is Processing Personal Data as evidenced in the Student Data Collection Notice and
  - (ii) RHSU shall be a Controller where it is Processing Personal Data as evidenced in its Privacy Notice published on its website
- (c) Notwithstanding Paragraph 2.1.1(b), 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 2.2.2(e) where Personal Data has been transmitted by it, or while Personal Data is in its possession or control.

2.1.2 Each of the Parties acknowledges and agrees that Paragraph 2.3 of this Agreement is an accurate description of the Data Processing Particulars.

## 2.2 Data Controller Obligations

- 2.2.1 Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.
- 2.2.2 Without limiting the generality of the obligation set out in Paragraph 2.2.1, in particular, each Party shall:
  - (a) where required to do so make due notification to the ICO;
  - (b) ensure it is not subject to any prohibition or restriction which would:
    - (i) prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
    - (ii) prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or
    - (iii) prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
  - (c) 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;

- (d) ensure that all Personal 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 either Party to Process the Personal Data as envisaged under this Agreement;
- (e) ensure that appropriate technical and organisational security measures are in place;
- (f) 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 2.2.2(f), 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;
- (g) 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;
- (h) notify the other Party in writing without undue delay and, in any event, within [twenty-four (24) hours] 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;
- (i) take reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data;
- (j) not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
- (k) not transfer any Personal Data it is processing to a Restricted Country;
- (l) 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; and
- (m) not disclose the Personal Data to a third party (including a sub-contractor) in any circumstances without the other Party's prior written consent, save in relation to: (i) disclosures to Permitted Recipients; and

(ii) Third Party Requests. For Third Party Requests, the Party seeking to disclose the Personal Data shall use reasonable endeavours to advise the other Party in advance of such disclosure, unless that Party is prohibited by law or regulation from notifying the other Party of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation).

### 2.3 Data Protection Particulars

The College will share the following Personal Data of prospective and enrolled students with RHSU:

- Name
- College Card number
- Date of birth
- Sex
- College email address
- Course (also known as degree programme)
- Department
- Year of study
- Home postcode

The College shares this data in accordance with both a legal obligation within the Education Act 1994, to which the College is subject, and also the legitimate interests of RHSU in order that they can fulfil their function and in the legitimate interests of the students so they can make use of RHSU's offering.

RHSU will share the following Personal Data of enrolled students with the College:

- Name and College card number of all students enrolled as a member in a student group (with the exception of where these groups pertain to special categories of data). RHSU shares this data in accordance with the legitimate interests of the College in order that they can conduct statistical research and analysis of student engagement with Sport.
- Name, College card number and number of passport points accumulated of all students who have earned passport points through Students' Union activities. RHSU shares this data in accordance with the legitimate interests of the College in order that they can administer Passport Points in the legitimate interests of the students in relation to their employability skills record.
- Name, College card number and term-time address of any students involved in Accidents or Incidents at any of the Students' Union venues. RHSU shares this data in accordance with a legal obligation with Health & Safety compliance and in the legitimate interests of the College and the students for welfare purposes.
- Name and College card number of a student whereby it is deemed necessary to break confidentiality for the protection of the vital interests of the student.