

Data Protection Agreement

This Agreement Dated: 14th September 2018

Between the Parties:

Canterbury Christ Church University ("The University") a registered Company with Company Number 04793659 and charity with Registered Charity Number 1098136 and ICO registration number Z7043317 whose registered office is at Rochester House, St Georges Place, Canterbury, Kent CT1 1UT.

And

Christ Church Students' Union ("the Union") a Registered Company with Company Number 07618194 and charity with registered Charity Number 1142619 and ICO registration number Z1111670 whose registered office is at St. George's Centre, St Georges Place, Canterbury, Kent CT1 1UT.

Introduction

The Union is a Students' Union as defined by s20 of Education Act 1994 as, "an association of the generality of students at an establishment to which this Part applies whose principal purposes include promoting the general interests of its members as students; or (b) a representative body (whether an association or not) whose principal purposes include representing the generality of students at an establishment to which this Part applies in academic, disciplinary or other matters relating to the government of the establishment."

The Union is a representative body of the Student Members that is recognised by the Governing Body of the University as an association of Students of the University.

The Union is a registered charity and a company limited by guarantee. The Union conducts and manages its own affairs and funds in accordance with a constitution approved by the Governing Body and is required to present its audited accounts annually to the Governing Body in accordance with the Financial Memorandum.

Data is shared between the University and the Union in order for the parties to carry out their respective duties imposed upon them under the Education Act 1994 and particularised in Appendix 1.

DATA PROTECTION

Each Party agrees to comply with its obligations as set out in Schedule 1 (Data Protection) of this Agreement.

I am authorised to sign this on behalf of the University:

Name: **Professor Helen James**

Position: **Senior Pro-Vice Chancellor Education, Enhancement & Student Experience**

I am authorised to sign this on behalf of the Union:

Name: **Ben MacPhee**

Position: **Chief Executive Officer**

SCHEDULE 1

DATA PROTECTION

1. DEFINITIONS

In this Schedule 1 the following definitions shall apply:

"Controller", "Processor" "Data Subject" and "Data Protection Officer"	shall have the meaning given to those terms in the applicable Data Protection Laws;
"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 2018 ("DPA") and 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;
"Data Processing Particulars"	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 Appendix 1.
"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;
"Good Industry Practice"	means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert Union seeking to comply with its contractual obligations in full and complying with all applicable laws including the Data Protection Laws;
"ICO"	means the UK Information Commissioner's Office, or any successor or replacement body from time to time;

"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;
"Personal Data"	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 Appendix 1 (<i>Data Processing Particulars</i>));
"Personal Data Breach"	has the meaning set out in the Data Protection Laws and for the avoidance of doubt , includes a breach of Paragraph 2.2.2(d);
"Processing"	has the meaning set out in the Data Protection Laws (and " Process " and " Processed " shall be construed accordingly);
"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 operating as a Students' Union for the benefit of all students at the University; and
"Third Party Request"	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. Notwithstanding the foregoing, 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 University shall be a Data Controller where it is Processing Personal Data in relation to carrying out its obligations as a University, and
 - (ii) the Union shall be a Data Controller where it is Processing Personal Data in relation to its obligations as a Students' Union.
 - (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(d) 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 Appendix 1 (*Data Processing Particulars*) to this Agreement is an accurate description of the Data Processing Particulars.
- 2.1.3 Each of the Parties acknowledges that:
- (a) the Data Protection Officer for the University is Robert Melville, 01227 922281 and dp.officer@canterbury.ac.uk; and
- the Data Protection Champion for the Union is Ben MacPhee, 01227 922109 and data@ccsu.co.uk.

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; For the avoidance of doubt the University does not warrant to the Union that any use of the Personal Data outside the scope of this Agreement shall be compliant 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 sufficient to comply with:
 - (i) at least the obligations imposed on the Controller by the Security Requirements; and

and where requested provide to the University evidence of its compliance with such requirements promptly, and in any event within forty-eight (48) hours of the request;

- (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;

Appendix 1

Data Protection Particulars

The subject matter, Purpose and duration of the Processing	<p>Subject matter and Purposes of Processing (both Parties have obligations under ss20-22 Education Act 1994);</p> <ol style="list-style-type: none"> 1. Managing Union membership, administration including managing the democratic process of electing Union representatives; 2. Managing membership of sports clubs and societies (legitimate interests of the Parties); 3. Managing members' volunteering opportunities (legitimate interest of the Parties). <p>Duration: for the duration of the data subject's membership of the Students' Union and retained for 3 years following the expiry of the Data Subject's Union membership.</p>
The nature of the Processing	<ul style="list-style-type: none"> • Data migration from University to Union and Union to University. • Soliciting and obtaining Personal Data. • Storing, recording, holding Personal Data. • Organising, adapting, altering Personal Data. • Retrieving, consulting, processing Personal Data. • Disclosing, transmitting, disseminating, making available Personal Data. • Erasing and destroying stored Personal Data.
The type of Personal Data being Processed	<p>The types/categories of Personal Data being Processed:</p> <p>Subject Matter 1: Union Membership</p> <ul style="list-style-type: none"> • Student ID number; • First names; • Last name; • Date of birth; • Gender; • Mode of attendance; • Programme name; • Year of study; • Level of study; • Faculty; • Department; • Campus; • University email address; • Student status (UK, EU or international). <p>Subject Matter 2: Clubs, societies, etc</p> <ul style="list-style-type: none"> • Student ID number; • First names; • Last name; • University email address; • Payments/fees paid; • Membership of sports club(s); • Membership of society(s). <p>Subject Matter 3: Volunteering:</p> <ul style="list-style-type: none"> • Student ID number; • First names; • Last name; • Contact Email Address; • Contact telephone number;

	<ul style="list-style-type: none"> • Volunteering Interests; • Skills.
<p>The categories of Data Subjects</p>	<p>Subject Matter 1: Union Membership The Personal Data concerns individuals who have applied in order to receive, have received or are receiving educational services directly and/or indirectly from the University who have not exercised their right to opt out of Union Membership (22(2)(c)(i) Education Act 1994 and who are therefore automatically enrolled as a member of the Students' Union.</p> <p>Subject Matter 2: Clubs, sports, societies etc Union members who have expressed an interest in sports, societies and any additional related services offered by the Union.</p> <p>Subject Matter 3: Volunteering: Union members who have expressed an interest in the volunteering opportunities available to members.</p>