**DATA SHARING AGREEMENT**

This Agreement is made on the later date of the signatures of both parties.

**PARTIES**

1. **CANTERBURY CHRIST CHURCH UNIVERSITY** incorporated and registered in England and Wales with company number 04793659 whose registered office is at Anselm, North Holmes Road, Canterbury, England, CT1 1QU **(CCCU)**.
2. **Christ Church Students' Union** incorporated and registered in England and Wales with company number 07618194 and charity with number 1142619 and ICO registration number Z1111670 whose registered office is at Mary Seacole, North Holmes Road, Canterbury, England, CT1 1QU **(the Union).**

**BACKGROUND**

1. The Union is a Students' Union as defined by s20 of Education Act 1994. 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 at the University.
2. 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.
3. The Data Discloser agrees to share, and the Data Receiver agrees to use the Personal Data on the terms set out in this Agreement and in order to carry out the duties imposed upon both parties under the Education Act 1994 and particularised in Appendix 1.

**THE PARTIES AGREE:**

**1. INTERPRETATION**

The following definitions and rules of interpretation apply in this agreement:

1.1 Definitions:

**"Agreed Purpose"** has the meaning given to it in clause 2 of this agreement.

**"Agreement"** this agreement, which is a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

**"Commencement Date"** has the meaning given at the beginning of the Agreement.

**"Controller, Processor, Information Commissioner, Data Subject and Personal Data, Processing"** and appropriate "technical and organisational" measures shall have the meanings given to them in the Data Protection Legislation.

**"Criminal Offence Data"** means Personal Data relating to criminal convictions and offences or related security measures to be read in accordance with section 11(2) of the DPA 2018 (or other applicable Data Protection Legislation).

**"Data Discloser"** means the party that provides Shared Personal Data relating to a Data Subject to the other party.

**"Data Receiver"** means the party that receives Shared Personal Data from the Data Discloser

**"Data Sharing Code"** the Information Commissioner's statutory data sharing code of practice which came into force on 5 October 2021, as updated or amended from time to time.

**"Deletion Procedure"** has the meaning given to it in clause 7.3.

**"Data Protection Legislation"** all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner and which are applicable to a party.

**"Governing Body"** means the arm of CCCU comprising its governors who are responsible for managing the university in accordance with laid

down regulations and promoting high standards of educational achievement in the university.

**"Personal Data Breach"** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data for the Agreed Purpose.

**"Shared Personal Data"** the Personal Data to be shared between the parties under this agreement.

**"Special Categories of Personal Data"** the categories of Personal Data set out in the Data Protection Legislation.

**"Student Member"** means a students who has not opted out of membership of the student union.

**"Subject Rights Request"** the exercise by a data subject of their rights under the Data Protection Legislation.

**"Supervisory Authority"** the Information Commissioner (ICO) or the relevant authority responsible for monitoring and enforcing data protection law in the United Kingdom at any given time.

**"Term"** the term of this Agreement as set out in clause 11.1.

1.1 This agreement is subject to the terms of the Student and University Partnership Agreement (the Master Agreement) and is hereby incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this agreement.

1.2 The Appendices form part of this agreement and shall have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Annexes.

1.3 In the case of any ambiguity between any provision contained in the body of this agreement and any provision contained in the Annexes, the provision in the body of this agreement shall take precedence.

1.4 A reference to writing or written includes email.

## 2. PERSONAL DATA TYPES AND PURPOSE

2.1 The parties consider this data sharing initiative necessary and proportionate as required to deliver the Services under the Master Agreement. The aim of the data sharing initiative is to enable the parties to fulfil their obligations under the Education Act 1994. It is fair as it will benefit students and the parties by providing educational support to students, and not unduly infringe their fundamental rights, freedoms and interests.

2.2 Appendix 1 describes the subject matter, duration, nature and purpose of the data sharing initiative and the Shared Personal Data categories and Data Subject types in respect of which the parties may process the Shared Personal Data.

2.2.1 The parties shall not Process Shared Personal Data including for the purposes of solely automated decision making producing legal effects or similarly significant effects, or otherwise in a way that is incompatible with the purposes described in this clause (Agreed Purpose).

2.3 Each party shall appoint a single point of contact (SPoC) who will work together to reach an agreement with regards to any issues arising from the data sharing and to improve actively the effectiveness of the data sharing initiative. The points of contact for each of the parties are:

2.3.1 Robert Melville, Data Protection Officer, dp.officer@canterbury.ac.uk and

2.3.2 Ben MacPhee, Data Protection Champion, data@ccsu.co.uk.

## 3. COMPLIANCE WITH NATIONAL DATA PROTECTION LAWS

3.1 Each party must always ensure compliance with applicable Data Protection Legislation during the Term of this agreement.

3.2 Each party has such valid registrations and has paid such fees as are required by the Information Commissioner or the prevailing national Supervisory Authority at any relevant time which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this Agreement, unless an exemption applies.

## 4. LAWFUL, FAIR AND TRANSPARENT PROCESSING

4.1 Each party shall ensure that it Processes the Shared Personal Data fairly and lawfully in accordance with clause 4.2 during the Term of this Agreement.

4.2 Each party shall ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal.

4.3 The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with Subject Rights Requests within the time limits imposed by the Data Protection Legislation.

4.4 The Data Receiver undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Data, the legal basis for such purposes and such other information as is required by the Data Protection Legislation including:

4.4.1 if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer; and

4.4.2 if Shared Personal Data will be transferred outside the UK or EEA pursuant to clause 8 of this agreement, that fact and sufficient information about such transfer, the purpose of such transfer and the safeguards put in place by the Controller to enable the Data Subject to understand the purpose and risks of such transfer.

**5. DATA QUALITY**

5.1 Shared Personal Data must be limited to the Personal Data described in Appendix 1 of this agreement.

**6. DATA SUBJECT'S RIGHTS**

6.1 The SPoC for each party is responsible for maintaining a record of Subject Rights Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The SPoC for each party are detailed in clause 2.3.

**7. DATA RETENTION AND DELETION**

7.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purpose.

7.2 Notwithstanding clause 7.1, parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry.

7.3 The Data Receiver shall ensure that any Shared Personal Data is returned to the Data Discloser or destroyed in accordance with the agreed Deletion Procedure set out in the following circumstances:

7.3.1 on termination of its involvement in this Agreement;

7.3.2 on expiry of the Term of this agreement; or

7.3.3 once Processing of the Shared Personal Data is no longer necessary for the purposes it was originally shared for, as set out in clause 2.2.

7.4 Following the deletion of Shared Personal Data in accordance with clause 7.3, the Data Receiver shall notify the Data Discloser that the Shared Personal Data in question has been deleted in accordance with this Agreement.

**8. TRANSFERS**

8.1 For the purposes of this clause, transfers of Personal Data shall mean any sharing of Personal Data by the Data Receiver with a third party, and shall include the following:

8.1.1 subcontracting the processing of Shared Personal Data;

8.1.2 8.1.2 granting a third party Controller access to the Shared Personal Data.

8.2 If the Data Receiver appoints a third party Processor to Process the Shared Personal Data it shall comply with the relevant provisions of the Data Protection Legislation and shall remain liable to the Data Discloser for the acts and/or omissions of the Processor.

8.3 The Data Receiver may only process, or permit the processing, of the Shared Personal Data outside the EEA under the following conditions:

8.3.1 it complies with the provisions of the Data Protection Legislation in the event the third party is a joint controller; and

8.3.2 it ensures that (i) the transfer is to a country approved under the applicable Data Protection Legislation as providing adequate protection; or (ii) there are appropriate safeguards or binding corporate rules in place pursuant to the applicable Data Protection Legislation; or (iii) the transferee otherwise complies with the Data Receiver's obligations under the applicable Data Protection Legislation by providing an adequate level of protection to any Shared Personal Data that is transferred; or (iv) one of the derogations for specific situations in the applicable Data Protection Legislation applies to the transfer.

**9. SECURITY AND TRAINING**

9.1 The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods as agreed and set out in Appendix 2.

9.2 The parties undertake to have in place throughout the Term of this agreement appropriate technical and organisational security measures to:

9.2.1 prevent:

9.2.1.1 unauthorised or unlawful processing of the Shared Personal Data; and

9.2.1.2 the accidental loss or destruction of, or damage to, the Shared Personal Data

9.2.2 ensure a level of security appropriate to:

9.2.2.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

9.2.2.2 the nature of the Shared Personal Data to be protected.

9.3 The level of technical and organisational measures agreed by the parties as appropriate as at the Commencement Date having regard to the state of technological development and the cost of implementing such measures is set out in Appendix 2. The parties shall keep such security measures under review and shall carry out such updates as they agree are appropriate throughout the Term of this agreement.

9.4 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in Appendix 2 together with any other applicable Data Protection Legislation and have entered into confidentiality agreements relating to the Processing of Personal Data.

9.5 The level, content and regularity of training referred to in clause 9.4 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and Processing of the Shared Personal Data.

## 10. PERSONAL DATA BREACHES AND REPORTING PROCEDURES

10.1 The parties shall each comply with its obligation to report a Personal Data Breach to the Information Commissioner or appropriate Supervisory Authority and (where applicable) Data Subjects under the Data Protection Legislation and shall each inform the other party of any Personal Data Breach irrespective of whether there is a requirement to notify the Information Commissioner or any Supervisory Authority or Data Subject(s).

10.2 The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

## 11. REVIEW AND TERMINATION OF THIS AGREEMENT

11.1 This agreement will remain in full force and effect so long as The Master Agreement remains in effect.

11.2 The parties shall review the effectiveness of this data sharing initiative every 12 months, having consideration to the aims and purposes set out in clause 2.1 and clause 2.2. The parties shall continue, amend or terminate this agreement depending on the outcome of this review.

11.3 The review of the effectiveness of the data sharing initiative will involve:

11.3.1 assessing whether the purposes for which the Shared Personal Data is being processed are still the ones listed in clause 2.3 of this Agreement;

11.3.2 assessing whether the Shared Personal Data is still as listed in Appendix 1 to this agreement;

11.3.3 assessing whether the legal framework governing data quality, retention, and data subjects' rights are being complied with; and

11.3.4 assessing whether Personal Data Breaches involving the Shared Personal Data have been handled in accordance with this Agreement and the applicable legal framework.

11.4 Each party reserves its rights to inspect the other party's arrangements for the Processing of Shared Personal Data and to terminate its involvement in this agreement where it considers that the other party is not Processing the Shared Personal Data in accordance with this agreement.

## 12. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE SUPERVISORY AUTHORITY

12.1 In the event of a dispute, complaint or claim brought by a Data Subject or the Information Commissioner or a Supervisory Authority concerning the

processing of Shared Personal Data against either or both parties, the parties will inform each other within a reasonable period of time about any such disputes, complaints or claims, and will cooperate with a view to settling them amicably in a timely fashion.

12.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner or by a Supervisory 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.

12.3 Each party shall abide by a decision of a competent court of the Data Discloser's country of establishment or of the Information Commissioner or a Supervisory Authority.

**13. WARRANTIES**

13.1 Each party warrants and undertakes that it will:

13.1.1 Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Personal Data processing operations.

13.1.2 Make available on request to the Data Subjects who are third party beneficiaries a copy of this agreement unless the Agreement contains confidential information.

13.1.3 Respond within a reasonable time and as far as reasonably possible to enquiries from the Information Commissioner or relevant Supervisory Authority in relation to the Shared Personal Data.

13.1.4 Respond to Subject Rights Requests in accordance with the Data Protection Legislation, including where necessary (i) advising the other party of any step(s) it should reasonably take in this regard; and (ii) where the legitimate ground relied upon is a Data Subject's consent, the timely operation of an effective procedure if such consent is withdrawn.

13.1.5 Where applicable, maintain registration with the Information Commissioner and all relevant Supervisory Authorities to process all Shared Personal Data for the Agreed Purpose.

13.1.6 Take all appropriate steps to ensure compliance with the security measures set out in clause 9 above.

13.2 The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Data to the Data Receiver and it will ensure that the Shared Personal Data is accurate.

13.3 The Data Receiver warrants and undertakes that it will not disclose or transfer the Shared Personal Data to a third-party Controller located outside the UK or EEA unless it complies with the obligations set out in clause 8.3 above.

13.4 Except as expressly stated in this agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the greatest extent permitted by law.

**14. NOTICE**

14.1 Any notice given to a party under or in connection with this agreement shall be in writing, addressed to the SPoCs and shall be:

14.1.1 delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

14.1.2 sent by email to the SPoC.

14.2 Any notice shall be deemed to have been received:

14.2.1 if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address;

14.2.2 if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume. In this clause 14.2.2, business hours means 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.

14.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

This agreement has been entered into on the date stated at the beginning of it.

**Signed by** Becky Huxley-Binns

for and on behalf of **CANTERBURY CHRIST CHURCH UNIVERSITY**

**Deputy Vice Chancellor and Provost**

**Signed by** Ben MacPhee

for and on behalf of **CHRIST CHURCH STUDENTS' UNION**

**Chief Executive Officer**

## APPENDIX 1

### Personal Data purposes and details

| | |
|---|---|
| Subject matter of data sharing | Both parties have agreed to share Personal Data in order to carry out their respective obligations under ss20-22 of the Education Act 1994, which |

| | |
|---|---|
| | include:<br><br>• managing Union membership, administration including managing the democratic process of electing Union representatives.<br><br>Other Purposes include:<br><br>• managing membership of sports clubs and societies.<br>• managing member's volunteering opportunities.<br>• Supporting students with complaint and disciplinary processes.<br>• Carrying out student member research using surveys. |
| Duration of data sharing | Personal Data is processed for the duration of the Data Subject's membership of the Union and retained for 3 years following the expiry of the Data Subject's Union membership. |
| Nature of sharing | **CCCU:**<br><br>The processes being done for the purpose of maintaining the relationship with the Data Subject and providing education services are:<br><br>• soliciting and obtaining Personal Data<br>• storing, recording, holding Personal Data<br>• organising, adapting, altering Personal Data<br>• retrieving, consulting, processing Personal Data<br>• disclosing, transmitting, disseminating, making available Personal Data<br>• manual entry, manipulation, and deletion of Personal Data<br>• automated entry, manipulation, and deletion of Personal Data, including automated backup, archive and deletion routines,<br>• erasing and destroying stored Personal Data<br>**CCSU**:<br><br>The processes being done for the purpose of maintaining the relationship with the Data Subject and providing educational services are:<br><br>• data migration from Union to University |

| | |
|---|---|
| | • soliciting and obtaining Personal Data<br>• storing, recording, holding Personal Data including a hard copy kept at the end of the Student Journey and processed in line with its Data Retention Policies<br>• organising, adapting, altering Personal Data<br>• erasing and destroying stored Personal Data<br>• disclosing, transmitting, disseminating, making available Personal Data. |
| Personal Data Categories | The type of Personal Data Processed include the following categories:<br><br>Non-sensitive Personal Data:<br><br>• Student ID number, First and Last names, 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, International), Personal email address, Contac telephone number, Membership of sports clubs, Membership of societies, Volunteering interests.<br><br>Sensitive Personal Data:<br><br>• Ethnicity data, Disability data, Sex life, Sexual Orientation data, Medical information (if relevant), Criminal Data (if relevant), any other special category data relevant to a student's general or academic misconduct/disciplinary case. |
| Data Subject Types | The Personal Data Concerns individuals who are:<br><br>• **Union Members:** 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, and who have NOT exercised their right to opt out of the Union membership (ss22(2)(c)(i) of the Education Act 1994 and who are therefore automatically enrolled as a member of the Student's Union.<br>• **Membership of Clubs, Sports, Societies etc:** Union members who |

| | |
|---|---|
| | have expressed an interest in sports, societies, and any additional related services offered by the Union.<br>• **Volunteering:** Union members who have expressed an interest in the volunteering opportunities available to members.<br>• **Student conduct and disciplinary:** Union members who have expressed an interest in having their rights advocated for during conduct and disciplinary procedures |

## APPENDIX 2

### Security measures

The parties have agreed to adhere to the technical and organisational data security measures below:

| | |
|---|---|
| Physical access controls | Each Party shall:<br><br>assign appropriate level of security based on a risk assessment.<br><br>have an information security policy (or equivalent) and take steps to make sure the policy is implemented.<br><br>ensure the information security policy (or equivalent) contains provisions relating to password use and physical storage of data. |
| System access controls | Each party shall have in place basic technical controls such as those specified by established frameworks like Cyber Essentials. |
| Data access controls | Each party shall make use of encryption and/ or pseudonymisation where it is appropriate to do so. |
| Transmission controls | Each party shall have policies that ensure that electronic transmission is carried out in a secure manner.<br><br>Transmission of sensitive data must be encrypted. |

| | |
|---|---|
| Input controls | Each party shall have technical controls in place to protect information assets, including:<br><br>The use of firewalls, anti-virus software, intrusion detection systems, and encryption. |
| Data backups | Each Party acknowledges the importance of confidentiality, integrity and availability for the Personal Data they process.<br><br>Each Party shall ensure that they can restore access to Personal Data in the event of any incidents, such as by establishing an appropriate backup process.<br><br>Each Party shall ensure that Personal Data is deleted at the end of its retention period, and Sensitive and Confidential Data is deleted using tools to wipe from disks and computer memory. |
| Data segregation | Each Party shall have an Information Classification Policy (or its equivalent) that assigns risk based on the nature of the Information and guides the use of information assets. |