UNIVERSITY OF CAMBRIDGE

THE UNIVERSITY, CAMBRIDGE IN AMERICA AND THE COLLEGES

DATA SHARING PROTOCOL

THIS PROTOCOL is dated 31 July 2023

BETWEEN

(1) The Chancellor, Masters, and Scholars of the University of Cambridge of The Old Schools, Trinity Lane, Cambridge, CB2 1TN (**University**).

(2) Cambridge in America of 1120 Avenue of the Americas, 17th Floor, New York, New York, 10036 (**CAm**).

(3) The 31 Cambridge Colleges as stated in Statute G of the *Statutes and Ordinances* of the University of Cambridge, contacted collectively through the Office of Intercollegiate Services Ltd., 12B King's Parade, Cambridge, CB2 1SJ (**Colleges**).

BACKGROUND

(A) The University and the Colleges work closely together as a collegiate university and with CAm (the **parties**) in relation to fundraising, student affairs and other matters. In relation to this Protocol, the University, the Colleges and CAm act through, or under the authority of, the University Council, Colleges' Committee and the CAm Board respectively.

(B) This Protocol sets out the responsibilities of each of the parties above in areas relating to the protection, security, sharing and processing of Personal Data that two or more of the parties require in order to conduct their individual or shared objectives and activities.

(C) This Protocol originated in 2018 and was last reviewed on the date shown above. It is intended to document arrangements for compliance with currently applicable Data Protection Laws as applicable to the parties.

IT IS AGREED AS FOLLOWS:

INTERPRETATION

1 The following definitions apply in this Protocol:

Agreed Purposes: has the meaning given to it in clause 5 of this Protocol.

Data Protection Authority: the UK Information Commissioner's Office (or any successor body).

Data Protection Laws: the UK General Data Protection Regulation (as defined in section 3(10) of the Data Protection Act 2018; **UK GDPR**), the Data Protection Act 2018, and any other applicable supplementary or successor legislation protecting Personal Data.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

Shared Personal Data: the Personal Data shared between the parties under clause 9 of this Protocol.

SPoC: a single point of contact of each signatory party, who is responsible for engaging with all elements of this Protocol.

2 **Data Controller**, **Joint Controllers**, **Data Processor**, **Data Subject** and **Personal Data**, **Sensitive Personal Data** or **Special Category Personal Data**, **processing** and **appropriate technical and organisational measures** shall have the meanings given to them in the applicable Data Protection Laws.

PURPOSE

3 This Protocol sets out the framework for the sharing of Personal Data between and among the parties as Data Controllers, Joint Controllers and as Data Processors.

4 The parties consider this data sharing necessary and in their mutual best interests as a collegiate university and not-for-profit organization. The aim of the data sharing is to ensure that each party's personal data records, admissions processes, academic processes, employment and membership processes, administration, alumni and supporter relations, and fundraising activities, amongst others, are carried out in a co-ordinated and efficient way. The parties acknowledge that CAm's role is limited to fundraising and alumni relations and so it will have more limited access to certain personal data and records.

5 To the extent the each party has access, the parties agree to process Shared Personal Data, as described in clause 9, only for and compatible with the following **Agreed Purposes**:

(a) Providing services to staff, students and others, including shared services; for the avoidance of doubt, this includes services the parties provide separately or jointly to staff, students and others as part of their wider duties and responsibilities, including health and wellbeing services and safeguarding services
(b) Maintaining current and historic academic and teaching records
(c) Administering admissions processes and records
(d) Staff and member administration and record-keeping
(e) Pursuing alumni and supporter relations, and fundraising activities
(f) Operating communications and IT infrastructure, including products used under licence by one or more of the parties
(g) Marketing
(h) Managing complaints, academic appeals, and disciplinary investigations, where the incident or substance requires input from one or more party
(i) Assessing the effectiveness of shared services
(j) Complying with legal and regulatory requirements and particularly where external agencies view the parties as a single entity
(k) Any other purpose incidental to or analogous with any of the above

6 Each party shall appoint a single point of contact (SPoC) who will work together to resolve any issues about and improve the effectiveness of the parties' data sharing. The parties will each ensure that the SPoC has a clear and up-to-date email address for communication purposes.

7 Any notice or other formal communication given to a party under or in connection with this Protocol shall be in writing, addressed to the SPoCs and shall be sent by email to the SPoC.

COMPLIANCE WITH APPLICABLE DATA PROTECTION LAWS

8 Each party must ensure compliance with applicable Data Protection Laws at all times.

SHARED PERSONAL DATA

9 Personal Data (including Special Category Personal Data) may be shared between the parties as necessary and where compatible with Data Protection Laws. The processing of Shared Personal Data must be relevant and proportionate with regard to the Agreed Purposes.

10 The parties agree wherever practicable to operate proportionate checks to ensure the accuracy of the Shared Personal Data and its correct incorporation into different systems at the time of data sharing. No party shall retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. Parties shall continue, however, to retain Shared Personal Data in accordance with any statutory retention periods applicable in their respective countries and/or states.

DATA SUBJECT RIGHTS

11 Each party shall, in respect of Shared Personal Data, ensure that their data protection statements (or privacy notices) are clear and that they provide sufficient information to the Data Subjects in accordance with applicable Data Protection Laws for them to understand what Personal Data is being shared with the other parties, the purposes of the data sharing, a contact point for the Data Subjects, and any other information to ensure that the Data Subjects understand how their Shared Personal Data will be processed. Each party shall retain and process the Shared Personal Data in accordance with the relevant data protection statement(s).

12 The parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with any rights requests, queries, or complaints from Data Subjects, in relation to the Shared Personal Data.

DATA PROCESSORS

13 In most cases, the data sharing is such that each party is a separate Data Controller, or are Joint Controllers, of the Shared Personal Data. For specific processing where one party acts only as the Data Processor for another (the Data Controller), the Data Processor shall ensure that it abides by the standards set out in the model data processor clauses issued by the University.

DIRECT MARKETING

14 If a party processes the Shared Personal Data for the purposes of direct marketing, that party shall ensure that:

(a) effective procedures and communications are in place to allow the Data Subject to exercise their rights not to receive direct marketing;

(b) effective procedures are in place to enable that party to advise other parties of any exercising of those rights that encompasses those other parties; and

(c) an appropriate legal basis has been confirmed (and, where necessary, evidenced) for the Shared Personal Data to be used for the purposes of direct marketing.

SECURITY AND TRAINING

15 Each party shall only provide and receive the Shared Personal Data using secure methods, having regard to the availability of joint or shared IT systems, the technology for facilitating data transfers, the risk of data loss or breach and the cost of implementing such measures. The parties shall share information about risk assessments with regard to the Shared Personal Data as necessary.

16 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 this Protocol.

DATA SECURITY BREACHES AND REPORTING PROCEDURES

17 The parties agree to provide reasonable assistance to each other to facilitate the handling of any Data Security Breach in an expeditious and compliant manner. Where the parties are joint controllers, the SPoCs shall determine on a case-by-case basis which party should take the lead on investigating and reporting any Data Security Breach.

18 The parties should report any relevant potential or actual losses of the Shared Personal Data and remedial steps taken, either through mechanisms specified by the parties from time to time or otherwise to each and every relevant SPoC as soon as possible, to enable the parties to consider what further action is required either individually or jointly.

ADDITIONAL PROVISIONS IN RELATION TO CAMBRIDGE IN AMERICA

19 Cambridge in America (CAm) is incorporated under the laws of the District of Columbia in the United States and is subject to its laws and other laws applicable in the United States concerning data processing, and CAm shall comply with those laws and shall comply with this Protocol to the extent it applies to CAm and to CAm UK.

20 Transfers of Personal Data to CAm from the other parties are made on the basis of Schedule 1.

REVIEW AND TERMINATION OF PROTOCOL

21 The nature of the arrangements between the parties is such that it is extremely unlikely that the Protocol will be terminated in its entirety. Should all parties unanimously wish to terminate the Protocol, a process to identify the future ownership of and confirm as necessary mutual rights to use any Shared Personal Data will be undertaken and completed prior to termination of the Protocol.

22 Where any of the parties ceases to be a separate legal entity, it shall:

(a) inform each and every SPoC in writing as soon as possible in order to draft and agree one or more written procedures for the deletion and/or return of any Shared Personal Data as necessary; and
(b) be removed from the Protocol.

23 Any additional legal entity that wishes to be part of this data sharing Protocol may submit a request in writing to the University's SPoC. The consent of each and every party is required in order for the additional party to be included into this Protocol together with completion of contractual adherence to this Protocol.

24 In the event that a party is removed from the Protocol or a new legal entity joins the Protocol in accordance with clauses 22 and 23, an amended and updated version of this Protocol will be drafted as soon as practicable and circulated to all other parties.

25 The parties shall review the effectiveness of this data sharing Protocol every five years, or upon the addition and removal of a party, or upon the request of one or more of the parties, having consideration to the Agreed Purposes set out in clause 5, and to current Data Protection Laws, and to any concerns raised at that time by one or more of the parties. The parties shall continue or amend the Protocol depending on the outcome of the review but in the meantime the Protocol shall continue in full force and effect.

26 Each party is responsible for their own legal compliance and self-audit. A party, however, reasonably may ask to inspect another party's or parties' arrangements for the processing of Shared Personal Data and may request a review of the Protocol where it considers that another party is not processing the Shared Personal Data in accordance with this Protocol, and the matter has demonstrably not been resolved through discussions between the relevant SPoCs.

CHANGES TO APPLICABLE DATA PROTECTION LAWS

27 Should the applicable Data Protection Laws change in a way that the Protocol is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the SPoCs will negotiate in good faith to review the Protocol in light of the new legislation but in the meantime the Protocol shall continue in full force and effect.

RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE DATA PROTECTION AUTHORITY

28 In the event of a dispute or claim brought by a Data Subject or a Data Protection Authority concerning the processing of Shared Personal Data against any or all parties, the parties will inform each other as necessary about the dispute or claim, and will cooperate with a view to settling the dispute or claim amicably in a timely fashion.

Approved on behalf of the University of Cambridge
by the University Council on 31 July 2023

Approved on behalf of Cambridge in America by the
CAm Board (acting through the Executive
Committee) on 12 July 2023

Approved on behalf of the Colleges by the Colleges'
Committee on 8 July 2023

Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The date of the Protocol	
The Parties	**Exporters (who send the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	University Colleges	CAm

Key Contact	The SPoCs of the University and each of the Colleges	The SPoC of CAm

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	YES	YES	NO			
2	N/A					
3	N/A					
4	N/A					

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Cambridge and the Colleges are the Exporters. CAm is the Importer.
Annex 1B: Description of Transfer: As set out in clauses 4, 5, 9 and 10 of the Protocol.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in clauses 15, 16, 17 and 18 of the Protocol.

Annex III: List of Sub processors (Modules 2 and 3 only): N/A.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporters ☐neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.