

DATED

2018

Cambridge Theological Federation

&

Westfield House

DATA SHARING PROTOCOL

THIS PROTOCOL is dated

2018

BETWEEN

- (1) The Cambridge Theological Federation of The Bounds, Westminster College, Lady Margaret Road, Cambridge, CB3 0BJ (the “**CTF**”)
- (2) Westfield House of 30 Huntingdon Rd, Cambridge, CB3 0HH (the “**House**”)

BACKGROUND

- (A) The CTF and the House (the **parties**) work closely together in relation to student affairs and other matters.
- (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 the parties require in order to conduct their individual or shared objectives and activities.
- (C) This Protocol is intended to document compliance with the General Data Protection Regulation ((EU) 2016/679) (GDPR). It does not address other commercial or operational issues.

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: a national authority, as defined in the GDPR: for the UK, this is the Information Commissioner’s Office.

Data Protection Legislation: the General Data Protection Regulation ((EU) 2016/679) (**GDPR**) and any applicable national 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 10 of this Protocol.

Subject Access Request: has the same meaning as “Right of access by the data subject” in Article 15 of the GDPR.

- 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 Legislation.

PURPOSE

- 3 This Protocol sets out the framework for the sharing of Personal Data between 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 theological education institutions. The aim of the data sharing is to ensure that each party’s personal data records, admissions processes, academic processes, employment and

membership processes, and administration, amongst others, are carried out in a co-ordinated and efficient way.

- 5 The parties agree to process Shared Personal Data, as described in clause 9, only for and compatible with the following **Agreed Purposes**:
- (a) Maintaining academic and teaching records
 - (b) Administering admissions processes and records
 - (c) Staff administration and record-keeping
 - (d) Tier 4 visa processing and related activities
 - (e) Operating communications and IT infrastructure
 - (f) Marketing
 - (g) Providing services to staff, students and others
 - (h) Managing complaints, academic appeals, and disciplinary investigations, where the incident or substance requires input from one or both parties
 - (i) Any other purpose incidental to or analogous with any of the above.
- 6 The Principal of each House and the President of the CTF shall act as the single point of contact (SPoC) who will work together to resolve any issues about and improve the effectiveness of the parties' data sharing.
- 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:
- (a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office; or
 - (b) sent by email to the SPoC.

COMPLIANCE WITH APPLICABLE DATA PROTECTION LEGISLATION

- 8 Each party must ensure compliance with applicable Data Protection Legislation at all times, including the principles and standards set out in the Schedule .

SHARED PERSONAL DATA

- 9 The following types of Personal Data may be shared between the parties:
- (a) Contact and biographical details
 - (b) Application and student records
 - (c) Staff records
 - (d) Financial records
 - (e) Records relating to the use of services
- 10 Special Category Personal Data and Sensitive Personal Data may be shared between the parties only where compatible with the Data Protection Legislation.
- 11 The processing of Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.
- 12 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.

DATA PROCESSING

- 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 complies with Article 28 of the GDPR.

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 right to opt out from direct marketing;
 - (b) effective procedures are in place to enable that party to advise other parties of any opt out 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.

DATA SECURITY BREACHES AND REPORTING PROCEDURES

- 15 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.
- 16 The parties should notify 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.

REVIEW AND TERMINATION OF PROTOCOL

- 17 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 both 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.
- 18 The parties shall review the effectiveness of this data sharing Protocol every five years or upon the request of one of the parties, having consideration to the aims and purposes set out in clause 5, and to current Data Protection Legislation, 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.
- 19 Each party is responsible for their own legal compliance and self-audit. A party, however, reasonably may ask to inspect another party 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.

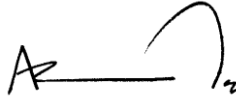
CHANGES TO APPLICABLE DATA PROTECTION LEGISLATION

- 20 Should the applicable Data Protection Legislation 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

21 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.

Signed by Alastair Oatey
for and on behalf of The CTF

A handwritten signature in black ink, appearing to be 'A Oatey', with a large, sweeping flourish above the name.

Signed by Cynthia Lumley
for and on behalf of Westfield House

.....

Schedule: Data protection principles and standards

LAWFUL AND FAIR PROCESSING

- 1.1 Each party shall commit to processing any Shared Personal Data lawfully, fairly and in a transparent manner and in accordance with the data protection principles in Article 5 of the GDPR.
- 1.2 Each party shall ensure that it processes Shared Personal Data under one or more of the legal bases in Article 6 of the GDPR and Data Protection Legislation.
- 1.3 In addition to its obligations under paragraph 1.2 of this Schedule 1, each party shall ensure that it processes Shared Personal Data classified as Special Category (Sensitive) Personal Data under one or more of the legal bases in Article 9 of the GDPR and applicable Data Protection Legislation.
- 1.4 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 Legislation 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 or process the Shared Personal Data in accordance with the relevant data protection statement(s).

DATA SUBJECTS' RIGHTS

- 1.5 Data Subjects have the right to obtain certain information about the processing of their Personal Data (including Shared Personal Data) through a Subject Access Request. In certain circumstances, as defined in the GDPR, Data Subjects may also request rectification, erasure or blocking of their personal data and may exercise other rights.
- 1.6 SPoCs should endeavour to maintain a record of individual requests from Data Subjects, including the decisions made and actions taken.
- 1.7 The parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other rights requests, queries or complaints from Data Subjects.

DATA RETENTION AND DELETION

- 1.8 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 TRANSFERS OUTSIDE THE EEA

- 1.9 For the purposes of paragraphs 1.10 and 1.11 of this Schedule 1, transfers of Personal Data shall mean any sharing of Personal Data outside the European Economic Area (EEA), and shall include, but is not limited to, the following:
 - (a) storing Shared Personal Data on servers outside the EEA.
 - (b) sub-contracting the processing of Shared Personal Data to data processors located outside the EEA.

- (c) granting third parties located outside the EEA access rights to the Shared Personal Data.

1.10 The parties shall only disclose or transfer the Shared Personal Data to a third party located outside the EEA in line with the provisions of Chapter V of the GDPR as implemented in the applicable Data Protection Legislation.

SECURITY AND TRAINING

1.11 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 facilitate data transfers, the risk of data loss or breach and the cost of implementing such measures.

1.12 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 any agreed technical and organisational measures to keep it secure and to uphold the data protection principles in Article 5 of the GDPR.