Data Processing Agreement

between

The Customer

and

Abacus Edutech Limited

CONTENTS

CLAUSE

1. *Definitions and Interpretation*
2. *Personal data types and processing purposes*
3. *Provider's obligations*
4. *Provider's employees*
5. *Security*
6. *Personal data breach*
7. *Cross-border transfers of personal data*
8. *Subcontractors*
9. *Complaints, data subject requests and third-party rights*
10. *Term and termination*
11. *Data return and destruction*
12. *Records*
13. *Audit*
14. *Warranties*
15. *Indemnification*
16. *Notice*

ANNEX

ANNEX A *Personal Data processing purposes and details.*
ANNEX B *Security measures*

This agreement becomes effective on the Commencement Date, in accordance with clause 1.4 of the accompanying Terms & Conditions

PARTIES

(1) The Customer

(2) Abacus Edutech Limited incorporated and registered in England and Wales with company number 13880209 whose registered office is at 22 Faulkner Place, Brize Norton, Carterton, United Kingdom OX18 1NF (the **Provider**)

BACKGROUND

(A) The Customer and the Provider entered into "Abacus Edutech Limited Terms and Conditions" (**Master Agreement**) on the Commencement Date that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give the Provider written personal data processing instructions and from whom the Provider agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified in Annex A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller: has the meaning given to it in section 6, DPA 2018.

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**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement, as specified in Annex A. Any information relating to an identified

or identifiable living individual which the Provider collects or holds as controller in its own name shall not fall within the definition of the term 'Personal Data' as used in this Agreement, and will instead be collected, stored and used by the Provider under the terms of the relevant privacy notice published by the Provider to relevant data subjects.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

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

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Records: has the meaning given to it in Clause 12.

Term: this Agreement's term as defined in Clause 10.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any Customer written instructions requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires the Provider to process or disclose the Personal Data to a third-party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner under the Data Protection Legislation.

3.5 The Provider must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of the Master Agreement or this Agreement.

4. Provider's employees

The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

5. Security

5.1 The Provider must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in ANNEX B.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 The Provider will within 48 hours and in any event without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Provider will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Cross-border transfers of personal data

7.1 The Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK without obtaining the Customer's prior written consent, which consent is hereby provided in respect of transfers of Personal Data to the subcontractors approved as at the commencement of this Agreement, as set out in Annex A.

8. Subcontractors

8.1 The Provider may not authorise any third party or subcontractor, other than the subcontractors approved as at the commencement of this Agreement, as set out in Annex A, to process the Personal Data, save in accordance with the remaining provisions of this clause 8.

8.2 The Provider may only authorise a third-party (subcontractor) to process the Personal Data if:

(a) the Customer is provided with an opportunity to object to the appointment of each subcontractor within 10 working days after the Provider supplies the Customer with full details in writing regarding such subcontractor;

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts;

(c) the Provider maintains control over all of the Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.3 Those subcontractors approved as at the commencement of this Agreement are as set out in Annex A. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.4 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider which contains terms substantially the same as those set out in this Agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.5 The Parties agree that the Provider will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within 5 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) the Provider retains any of the Personal Data related to the Master Agreement in its possession or control (Term).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Provider without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 60 days, either party may terminate the Master Agreement on not less than 20 working days' written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Provider will, if requested by the Customer, securely delete or destroy all or any of the Personal Data related to this Agreement in its possession or control. In the absence of such request, the Customer acknowledges that the Provider may retain Personal Data related to this Agreement in back-up archives in accordance with the Provider's data retention policy, and may use such Personal Data in accordance the description of processing activities in Annex A, including for purposes of testing the functionality of the systems used by the Provider in the delivery of scheduling services to its customers. The Provider will in any event delete all Personal Data related to this Agreement in its possession or control within 90 days of termination of the Master Agreement for any reason or expiry of its term, subject to the provisions of clause 11.3.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 14 days after it completes the deletion or destruction.

11.5 The Customer acknowledges that it remains the Customer's obligation to ensure that any Personal Data which the Provider processes on the Customer's behalf is retained and used in accordance with the requirements of Data Protection Legislation, and in accordance with the Customer's privacy notices and data retention policy. The solution provided by the Provider pursuant to the Master Agreement permits the Customer to amend and delete Personal Data from the Provider's systems, and the Customer is responsible for using such functionality in order to comply with its obligations under this Clause 11.5.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (Records).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Data Protection Legislation and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 The Provider will permit an independent third-party auditor appointed by the Customer and approved by the Provider (such approval not to be unreasonably withheld) (the **Independent Auditor**) to audit the Provider's compliance with its obligations under this Agreement, on at least 60 days' notice, during the Term. The Provider will give the Independent Auditor all necessary assistance to conduct such audits at no additional cost to the Customer.

13.2 The Customer will treat any audit reports created by the Independent Auditor as the Provider's confidential information under the Master Agreement.

13.3 The Provider will promptly address any exceptions noted in the audit reports created by the Independent Auditor with the development and implementation of a corrective action plan by the Provider's management.

14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

15.2 Any limitation of liability set forth in the Master Agreement will apply to this Agreement's indemnity or reimbursement obligations.

16. Notice

Any notice or other communication given to a party under or in connection with this Agreement must be in writing and issued in accordance with clause 11.9 of the accompanying Terms & Conditions.

This Agreement has been entered into on the Commencement Date, in accordance with clause 1.4 of the accompanying Terms & Conditions.

ANNEX A Personal Data processing purposes and details

The Controller authorises the Processor to process the below defined Personal Data for the provision of the TA Timetabler product.

TA Timetabler is a web-based application to help schools efficiently manage the scheduling of their teaching assistants.

The purpose of this Annex is to define the specific details of the Processing of Personal Data. The provisions of the Data Processing Agreement between the Parties shall apply.

1. Data Subjects. The Personal Data transferred concern the following categories of Data Subjects:
    - 1.1. **Students**
    - 1.2. **School staff** (teaching and support staff)

2. Categories of Data. The Personal Data transferred concern the following categories of data:
    - 2.1. **Required Student data** - to include pupils on roll - *not pre-admission students*
        - 2.1.1. Name
        - 2.1.2. Year group
        - 2.1.3. Registration group
        - 2.1.4. House group
        - 2.1.5. SEN Status - *commonly used by users to identify students that need TA support*
        - 2.1.6. SEN Codes - *commonly used by users to identify students that need TA support*
        - 2.1.7. Student UPN - *used to match student records imported by users*
        - 2.1.8. Subjects studied
        - 2.1.9. Academic class memberships
        - 2.1.10. Timetable information
    - 2.2. **Optional Student data** - not pre-admission students. *Most of these fields are displayed to users to help them identify which students require support.*
        - 2.2.1. Legal name - *only used if "Name" components are missing/incomplete*
        - 2.2.2. Gender
        - 2.2.3. In LEA care
        - 2.2.4. Family in service
        - 2.2.5. Child protection plan
        - 2.2.6. Pupil premium eligibility
        - 2.2.7. Free school meals eligibility
        - 2.2.8. EAL
        - 2.2.9. First Language
        - 2.2.10. Gifted and talented status
    - 2.3. **Optional Pre-admission Student data**. *Pre-admission students are used to schedule Teaching Assistant support for incoming year 7 students before the start of a new academic year.*
        - 2.3.1. Name
        - 2.3.2. Legal name - *only used if "Name" components are missing/incomplete*

2.3.3. Year group (if available)
2.3.4. Registration group (if available)
2.3.5. House group (if available)
2.3.6. Gender
2.3.7. SEN Status
2.3.8. SEN Codes
2.3.9. Student UPN - used to match student records imported by users
2.3.10. In LEA care
2.3.11. Family in service
2.3.12. Child protection plan
2.3.13. Pupil premium eligibility
2.3.14. Free school meals eligibility
2.3.15. EAL
2.3.16. First Language
2.3.17. Gifted and talented status

2.4. Required Staff data

2.4.1. Name
2.4.2. Staff initials/Staff Code
2.4.3. Email address - *enables users to email timetables to staff members*
2.4.4. Dates of employment - *used to identify active staff members and prevent inactive staff being incorrectly assigned to lessons they cannot cover. TA Timetabler allows future staff members to be scheduled in advance*
2.4.5. Timetable and availability information

2.5. Optional Staff data

2.5.1. Legal name - *only used if "Name" components are missing/incomplete*

3. Nature and purpose of processing

3.1. All student and staff data that is processed is done so with the ultimate business aim of the efficient scheduling of teaching assistants, which may include the use of such data for purposes of testing the functionality of the systems used by the Provider in the delivery of such scheduling services to its customers.

3.2. Student data is processed to allow the easy identification of which classes and lessons require the allocation of additional teaching assistant support.

3.3. Staff data is processed to identify the suitability and availability of teaching assistants for allocation to identified classes and lessons, and to assign teaching assistants to these lessons. It is also used to enable sending timetables to staff members by email.

4. Duration of processing. The Provider will process the above data only for as long as the Master Agreement remains in effect, or for such longer period as may be permitted in accordance with clause 11 (Data Return and Destruction).

Approved Subcontractors:

The following entities have been appointed by the Provider as sub-processors in respect of Personal Data processed under this Agreement:

Sub-processor	**Location of processing**	**Processing activities**
MS Azure	UK	Cloud storage and web hosting
Brevo (together with its subprocessors described in the Brevo DPA - https://www.brevo.com/legal/termsofuse/)	International locations – as described in the Brevo DPA - https://www.brevo.com/legal/termsofuse/	Email Service. Names and email addresses of staff members/users are used to send emails as part of the function of TA Timetabler. Important information about TA Timetabler and Abacus Edutech may be sent to users from time to time. No student data is processed by Brevo, although some student details could be in the content of the emails generated by users.
CloudMersive (together with its subprocessors described in the Cloudmersive DPA - https://cloudmersive.com/data-processing-dpa)	The United States and any other country in which Cloudmersive or any of its Subprocessors maintains facilities – as described in the Cloudmersive DPA - https://cloudmersive.com/data-processing-dpa	Online virus scanner. In some cases, users may choose to upload files to Abacus Edutech servers through TA Timetabler. CloudMersive performs a virus check on these files and does not at any time persist the data on its servers

Interfacing Third Parties

The Customer authorises the Provider to liaise with Wonde Limited and/or such other providers of school data management services as the Provider may work with from time to time (each, an **Interfacing Third Party**) to implement the necessary data flows required for the provision of the Service to the Customer.

The Customer is responsible for ensuring that the Provider is given permission to access the required information through its administration of the Wonde API (or the API of any relevant Interfacing Third Party).

The Customer acknowledges that any processing of Personal Data by an Interfacing Third Party in connection with the provision of the Services to the Customer is undertaken pursuant to the terms of the data processing agreement

in effect between the Customer and the Interfacing Third Party, notwithstanding that the instructions (whether communicated via API or otherwise) given to the Interfacing Third Party in respect of such processing may be given by the Provider acting on the Customer's behalf.

The Customer acknowledges that the Provider is not responsible for the Customer's arrangements with the Interfacing Third Party, or the accuracy of any data provided by the Interfacing Third Party to the Customer.

ANNEX B Security measures

Adoption of standards

The Provider holds, and shall maintain during the Term, Cyber Essentials accreditation.

System access controls

Only the directors of the Provider have access to the system administrator dashboard. Access is secured by OAuth 2.0 and two-factor authentication.

Data access controls

Only the directors of the Provider can access the data. Data is stored in an encrypted database within Microsoft Azure Cloud.

Transmission controls

All data is encrypted in transit.

Data backups

Data is backed up regularly using Microsoft Azure Cloud backup mechanisms. All backups are encrypted.

Data segregation

Customers can only see data relating to their organisation. They cannot access data from other organisations.