Data Processing Agreement ("DPA")

SECTION A – COMPANY DETAILS

Each referred to as a **"Party"** and together the **"Parties"**.

Full Legal Name:	Get Set 4 Education Ltd ("GS4E")
Registration Number (if applicable):	ZA790560
Primary Contact Name and Title:	Natalie Richardson
Postal Address for Notices:	Get Set 4 Education Ltd Conifer House Yewlands Hoddesdon Herts EN11 8BX
Email Address for Notices:	admin@getset4education.co.uk

SECTION B – DETAILS OF DATA PROCESSING

Agreed Purpose of Processing:	To provide you (our customer) with a teaching and assessment tool on an online platform.
Commencement Date:	The date of the Contract with you (as defined in our terms and conditions)
Duration of Processing:	The duration of the Contract plus any further period of time that is required by law or due to a legal obligation.

Categories of Personal Data:	• Identity data • Contact data • Optional: Gender, PP, SEND, EAL information • Optional: Assessment information • Optional: Club and competition attendance information • Optional: Notes, photographs and videos of pupils
Categories of Data Subject:	• Staff • Optional: Pupils

SECTION C – TERMS AND CONDITIONS OF THE AGREEMENT

1. INTERPRETATION

1.1. The information contained in Sections **A** and **B** of this DPA constitute definitions for the purposes of this DPA and form part of this DPA. In addition, the following definitions, and rules of interpretation in this clause apply in this DPA. Definitions in GS4E's standard terms and conditions are also adopted in this DPA.

2. DEFINITIONS

2.1. **"Data Controller", "Data Processor", "Data Subject", "Personal Data", "Processing"** and **"Data Protection Impact Assessment"** shall have the meanings given in Applicable Data Protection Law;

"Applicable Data Protection Law" means 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); and 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.

2.2. **"Data"** means the Personal Data of GS4E's customers, their employees and/or students of GS4E's customers (if applicable) , where such Personal Data is processed under this DPA.

3. BACKGROUND

3.1. Data Controllers are liable for their compliance with Applicable Data Protection Law and must only appoint Data Processors who can provide 'sufficient guarantees' that the requirements of Applicable Data Protection Law will be met, and the rights of data subjects protected.

3.2. This DPA sets out the framework for the processing and/or sharing of Personal Data between the Data Controller and Data Processor and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

3.3. Nothing documented herein shall relieve any Data Controller of its own direct responsibilities and liabilities under any Applicable Data Protection Law of the European Union or United Kingdom to which they are subject.

4. THE PERFORMANCE OF DATA PROCESSING ACTIVITIES

4.1. The Data Processor shall process the Data as necessary to perform its obligations under the Contract and in accordance with the documented instructions of the Data Controller (the "**Agreed Purposes**")in this DPA, except where otherwise required by any law applicable to the Data Controller. In no event shall the Data Processor process the Data for its own purposes or those of any third party.

4.2. The Data Processor must promptly notify the Data Controller if, in its opinion, the Data Controller's instructions do not comply with the Applicable Data Protection Law.

5. INTERNATIONAL DATA TRANSFERS

5.1. The Data Processor will not transfer any of the Data that relates to children (nor permit any such data to be transferred) outside of the United Kingdom or the EEA.

5.2. Where any Data is transferred from the UK to the EEA, that is done on the basis of there being an adequacy decision in respect of the EEA. Should the EEA no longer be deemed adequate then the Data Processor will cease as soon as possible any data transfers to the EEA, or put in place other measures to ensure that such transfer is lawful and the Data is adequately protected.

5.3. Save to extent prohibited in clause 5.1 of this DPA, the Data Processor may transfer data outside of the UK and/or EEA provided always that such transfer complies with the requirements of Applicable Data Protection Laws, including ensuring an adequate level of protection for the Data and Data Subjects. This obligation includes ensuring compliance with Chapter 5 of UK GDPR.

6. ENSURING A DUTY OF CONFIDENCE

6.1. The Data Processor shall ensure that any entity or person that it authorises to process the Data (including its staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a

duty of confidentiality. The Data Processor shall ensure that all Authorised Persons process the Data only as necessary for the Agreed Purposes.

7. ENSURING THE SECURITY OF PROCESSING

7.1. The Data Processor shall, having regard to the nature of the Services, purposes of the Processing, potential risks and potential severity of harm to Data Subjects, implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, and loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**").

8. ENGAGEMENT OF SUB-PROCESSORS

8.1. The Data Processor shall not subcontract any processing of the Data to a third-party subcontractor without the prior written consent of the Data Controller, save for the those sub-processors identified at **Annex 1** which are deemed approved by the Data Controller. If the Data Controller refuses to provide its written consent to the Data Processor's appointment of a third-party subcontractor on reasonable grounds relating to the protection of the Data, then the Data Processor will not appoint the subcontractor.

8.2. Annex 1, being the list of approved sub-processors, shall include at least the names or categories of those sub-processors, the location of their processing, the services they provide to the Data Processor.

8.3. Where the Data Processor appoints a sub-processor, it will ensure that the sub-processor is bound by obligations equivalent to those contained in this DPA in respect of any processing of Personal Data. The Data Processor shall remain fully liable to the Data Controller for the performance and actions of any sub-processor.

9. EXERCISING DATA SUBJECT RIGHTS

9.1. The Data Processor shall so far as technically practicable provide all reasonable and timely assistance to the Data Controller to enable the Data Controller to respond to:

a) Any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and

b) Any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Data Processor, the Data Processor shall inform the Data Controller as soon as reasonably practicable providing reasonable details of the same.

10. ASSISTING THE DATA CONTROLLER TO MEET THEIR LEGAL OBLIGATIONS

10.1. If the Data Processor believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall inform the Data Controller as soon as reasonably practicable and provide the Data Controller with all such reasonable assistance as the Data Controller may reasonably require in order to conduct a Data Protection Impact Assessment (DPIA).

10.2. Upon becoming aware of a Security Incident, the Data Processor shall inform the Data Controller without undue delay and shall provide all

such timely information and cooperation as the Data Controller may reasonably require in order for the Data Controller to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law.

10.3. The Data Processor shall further take all such measures and actions as are technically practicable given the nature of the Services and within its control to remedy or mitigate the effects of the Security Incident and shall keep the Data Controller up-to-date about all developments in connection with the Security Incident.

10.4. The Data Processor shall notify the Data Controller as soon as reasonably practical of any legally binding request it receives from law enforcement unless such disclosure is prohibited.

10.5. The Data Processor shall maintain complete and accurate records and information to demonstrate its compliance with this DPA and provide the same promptly on request.

10.6. Upon the Data Controller's written request with reasonable notice given, within normal working hours, once per annum the Data Processor will permit a data protection audit in respect of the Data Controller, including locations at or from which the Services are provided by Auditors. During each audit, the Data Processor will grant the Auditors reasonable access to relevant books, records, systems, facilities, controls, processes and procedures to the extent related to a reasonable assessment of the Data Processor's data protection procedures and without compromising the confidentiality of itself or any other customer. The Data Processor will, in a timely manner, cooperate so far as is reasonable with the Auditors. The Data Controller shall use reasonable endeavours to procure that Auditors will seek to avoid disrupting the Data Processor's normal business operations during any audit. The Auditors shall not seek access to information or data belonging or relating to any

other customer of the Data Processor or which does not relate to the Services.

11. TERMINATION AND RETENTION OF DATA

11.1. Upon termination or expiry of this DPA, the Data Processor shall (at the Data Controller's election) securely destroy or return to the Data Controller all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that the Data Processor is required by any applicable law or by virtue of any other lawful grounds to retain some or all of the Data, in which event the Data Processor shall isolate and protect the Data from any further processing except to the extent required by such law.

11.2. The Data Processor shall not be in breach of this Clause if it acts on the instructions of the Data Controller.

11.3. The Data Processor acknowledges and agrees that the Data Controller retains all right, title and interest in and to the Personal Data.

ANNEX 1

Appointed Sub-processors:

Sub-Processor Name/Category:	Description of Services Provided:	Geographical Processing Location:	Where outside the UK, describe the legal safeguards in place:
Avamae	Software development and support	UK	NA
Stripe	Payment processor	UK	NA

Mailchimp	Marketing	USA	Mailchimp employs robust security measures and legal mechanisms to protect customers' data, security to safeguard information, maintain GDPR compliance, and ensure up to date certification mechanisms.
Wonde	Integration tool (optional)	UK	NA
Xero	Third party payment provider for invoices	USA	Xero transfers data to AWS's servers in the U.S., in compliance with EU data protection laws including Standard Contractual Clauses under the General Data Protection Regulation (GDPR).
Virtual Assistant	Administrative assistant services	Philippines	Transfer risk assessment, approved form international data transfer agreements and contractual obligations in place with any relevant virtual assistant. Processing is only of customer contact data and access to data is only through VPN, with data staying within GS4E environment. No processing is undertaken by this category of sub-processor in relation to children's personal data.
Helen Nicholas Accounting	Bookkeeping service	UK	NA