Data Processing Agreement

This Data Processing Agreement ("DPA") is incorporated by reference into the Terms of Service (as defined below) between Grupop.ie Limited (the "Provider") and the School (the "Customer").

IT IS AGREED as follows:

1. **Definitions**
   1.1. "**Terms Defined in Terms of Service**": Capitalised terms used in this DPA shall, unless otherwise defined herein or the context otherwise requires, have the meaning given to them in the Terms of Service.
   1.2. "**GDPR Terms**": The terms 'personal data', 'processor', 'controller', 'data subject', 'processing' and other terminology and definitions as used in the GDPR shall have the meanings given to them in the GDPR, unless otherwise defined herein.
   1.3. "**Data Protection Requirements**" means all legislation and regulations relating to the protection of personal data processed under the terms of this DPA and to which the Provider is subject including (without limitation) the Irish Data Protection Act 2018, the GDPR and all other applicable legislation;
   1.4. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
   1.5. "**Terms of Service**" means the terms of service, and any agreement entered into between the Customer and the Provider relating to the Services;
   1.6. "**SCCs**" means the standard contractual clauses approved by the EU Commission by Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries.
   1.7. **"Services"** means the digital educational tool known as Grupop and any other products or services the Provider may provide.

2. General
   2.1. In providing the Services, the Provider may process personal data on the Customer's behalf. The parties enter into this DPA to meet their obligations under Data Protection Requirements in respect of that processing.
   2.2. This DPA forms part of the Terms of Service. In the event of any conflict between this DPA and any other term of the Terms of Service relating to data protection or Data Protection Requirements, the terms of this DPA shall prevail.
   2.3. Severability: If the whole or any part of a provision of this DPA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity or enforceability of the remainder of the provision in question or any other provision of this DPA.

2.4. Binding on Successors: This DPA and all of its provisions shall be binding upon and inure to the benefit of the parties and their respective heirs, executors, administrators, successors and permitted assigns.

2.5. Survival of Obligations: The provisions of this DPA shall, as necessary, survive the termination of the provision of Services by the Provider however it arises, and shall continue to bind the parties or the relevant party (as applicable) without limit in time.

3. Obligations of the Parties

3.1. The details of the processing, the categories of personal data, the purposes and duration of processing for which the personal data is processed on behalf of the Customer are as set out in **Annex I.**

3.2. Status of Parties: For the provision of Services under the Terms of Service, Provider and Customer agree that Customer is the Controller and Provider is the Processor in respect of the personal data processed on behalf of the Customer.

3.3. Data Processor's Obligations: The Provider shall:

3.3.1. Only process Personal Data in accordance with the instructions of the Customer, which instructions shall be documented in writing by way of this DPA or Terms of Service;

3.3.2. Ensure that processing of Personal Data by it shall be carried out in compliance with Data Protection Requirements;

3.3.3. Inform the Customer immediately if, in its opinion, it receives an instruction from the Customer which infringes Data Protection Requirements;

3.3.4. Grant access to the personal data undergoing processing to members of its personnel only to the extent necessary for the exercise of its rights, and performance of its obligations, under this DPA and the Terms of Service. The Provider shall ensure that persons authorised to process the personal data have committed themselves to confidentiality.

3.3.5. Upon reasonable written request from Customer, provide to Customer such information as may be reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and allow for and contribute to audits, including inspections, conducted by the Customer or an audit managed by the Customer.

4. International transfers

4.1. Any transfer of data to a third country or an international organisation by the Provider shall be done only on the basis of documented instructions from the Customer or in order to fulfil a specific requirement under Union or Member State law to which the Provider is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

4.2. The Customer agrees that where the Provider engages a sub-processor in accordance with Clause 5.2 for carrying out specific processing activities (on behalf of the

Customer) and where those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Provider and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679 (SCCs), provided the conditions for the use of those standard contractual clauses are met.

4.3. Where the Customer is based outside the EU, UK and Switzerland, the Provider and Customer agree that any applicable transfers shall be governed by SCCs, which are incorporated by way of reference.

5. Sub-processors

5.1. The Provider has the Customer's general authorisation for the engagement of sub-processors as listed in Annex I and on request. The Provider shall inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least (where practical) 30 days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

5.2. Where the Provider engages a sub-processor for carrying out specific processing activities (on behalf of the Customer), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The Provider shall ensure that the sub-processor complies with the obligations to which the Provider is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

5.3. At the Customer's request, the Provider shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

5.4. The Provider shall remain fully responsible to the Customer for the performance of the sub-processor's obligations in accordance with its contract with the processor. The Provider shall notify the Customer of any failure by the sub-processor to fulfil its contractual obligations.

5.5. The Provider shall agree a third party beneficiary clause with the sub-processor whereby – in the event the Provider has factually disappeared, ceased to exist in law or has become insolvent – the Customer shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6. Data Breach

6.1. The Provider will notify the Customer without undue delay and within 72 hours after becoming aware of a Personal Data Breach in relation to the Services provided by the Provider and will use reasonable efforts to assist the Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

6.2. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained; and

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

7. Security of processing

7.1. The Provider shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

8. Data Subject Requests and Complaints

8.1. The Provider shall promptly notify the Customer of any request or complaint from a data subject.

8.2. The Provider shall not respond to the request or complaint itself unless authorised to do so by the Customer.

8.3. The Provider shall, on request of the Customer, taking into account the nature of the processing, reasonably assist the Customer in fulfilling its obligations to respond to data subjects.

9. Return or deletion of Personal Data

9.1. Following termination of the DPA, the Provider shall, at the choice of the Customer, delete all personal data processed on behalf of the Customer and certify to the Customer that it has done so or return all the personal data to the Customer and delete existing copies unless legal obligations require storage of the personal data.

10. Term and Termination

10.1. This DPA shall continue in full force and effect until the termination or expiry of the Terms of Service whereupon the Provider's authority to process Personal Data in accordance with this Agreement shall terminate automatically, unless otherwise agreed between the parties in writing.

Annex I

Description of the processing

- **Subject-Matter of Processing**: Processing of Personal Data as necessary for the provision of the Services
- **Duration of processing**: From the commencement of the Services until the Termination Date and for the purposes of the provision of Services
- **Categories of data subjects**:
  - Authorised Users (which includes Customer employees, contractors and other representatives, including teachers)
  - Pupils
- **Types of personal data to be processed**:
  - Pupil data includes the following:
    - Pupil first name only
    - Avatar customisation choices (predefined digital illustrations provided by Grupop — no pupil photos or images)
    - Group membership within the class
    - Pop count (reward progress)
  - Configuration data for teacher resources, pupil's internal ID, the class ID, the teacher's ID, the type of action (e.g. pupil removed, name corrected), and the date/time (timestamp)
- **Nature of the processing**:
  - The Provider processes the personal data on behalf of the Customer to provide the Services agreed upon in the Terms of Service
- **Purpose of the processing**:
  - Fulfilment of the Provider's obligations to provide the Services in accordance with the Terms of Service
- **Sub-processors:**
  - Microsoft Azure — cloud hosting, database storage, and file storage (servers located in West Europe)
  - Stripe — payment processing for teacher subscriptions (Stripe's privacy policy applies to payment data)

Annex II Technical and Organisational Measures (TOMs)

- Zero-Knowledge architecture — Grupop cannot itself identify pupils from the data held within the platform
- Pseudonymisation and encryption of personal data
- Data minimisation by design, so that only the data necessary to provide the service is collected
- Role-based access controls, limiting access to those who require it
- EU-based hosting with reputable infrastructure providers
- Due diligence and data processing agreements with all suppliers
- Annual archiving and deletion of class and pupil data
- Audit trails of key actions within the platform (for example, pupil removed or name corrected)
- Passwords are stored using industry-standard hashing (never in plain text)
- Data is stored on Microsoft Azure infrastructure which maintains its own extensive security certifications
- Microsoft Defender for Storage is enabled on our file storage to detect and prevent malicious uploads
- Personal data will only be processed by third parties on our instructions. Third parties are subject to appropriate data protection, security and confidentiality terms