Accelerus XUNO Data Processing Agreement (EU/UK GDPR)

This Data Processing Addendum ("DPA") is incorporated into and forms part of the Accelerus License Conditions ("License Conditions") between Semaphore Consulting Pty Ltd (trading as Semaphore Consulting), a company registered in Australia under with Australia Business Number 79 007 089 661 with its registered office at Suite 18, 79 Mahoneys Rd, Forest Hill, Victoria, Australia 3131 ("Semaphore Consulting") and you, the customer ("you", "your" or the "Customer"). It sets out the terms governing the processing of personal data in connection with the services provided under the Agreement. This DPA applies to the extent that Semaphore Consulting processes personal data on behalf of the Customer and ensures compliance with applicable data protection laws.

1. General

1.1. Customer is contracting with the Semaphore Consulting for it to process certain types of Personal Data on behalf of the Customer in accordance with this Data Processing Agreement and Applicable Privacy Laws.

1.2. The Data Processing Agreement is entered into within the context of the License Conditions and will be valid throughout the duration of the License Conditions as well as beyond insofar as it is necessary to ensure that Semaphore Consulting (and any Subprocessors) only process Personal Data provided by the Customer in accordance with this Agreement.

1.3. If there are any conflicts between the provisions of the Data Processing Agreement and the provisions of the License Conditions, the provisions of the Data Processing Agreement will take precedence.

1.4. The Agreement is subject to the GDPR, more specifically, the relevant contractual terms required of Processors and Controllers (Articles 28, 32 and 33 of the GDPR) and all applicable national and/or local legislation regarding data protection.

2. Processing Obligations

2.1. When processing Customer Personal Data, Semaphore Consulting shall carry out the following responsibilities:

2.1.1. Only process the Personal Data as specified in this Agreement, or as specified in any future written instructions of the Data Controller or as required by all Applicable Privacy Laws.

2.1.2. Inform the Customer if, in its opinion, an instruction infringes the Applicable Privacy Laws. The processing of the Personal Data required in said instruction shall be delayed until the Customer shall make a determination regarding how to process the Personal Data required in a manner consistent with Applicable Privacy Laws.

2.1.3. Guarantee that all personnel with access to Customer Personal Data are legally bound by confidentiality obligations not to disclose any Personal Data during and after the termination of the Agreement, including after the termination of their employment.

2.1.4. Assist the Data Controller, insofar as this is possible, to respond to any Data Subject's request exercising their rights in accordance with Chapter III of the GDPR.

2.1.5. Upon request, assist the Customer to comply with its obligations under the GDPR or other Applicable Privacy Laws when related to the processing of the Personal Data, including but not limited to security of processing, breach notifications, impact assessments and consultations and co-operation with supervisory authorities or regulators. Semaphore Consulting shall notify the Customer of any request of complaint received from the data subject related to the processing of Personal Data under this Agreement.

2.1.6. At the Customer's discretion, Semaphore Consulting shall return or irrevocably delete or remove the Personal Data upon termination of the Agreement, unless storage of the Personal Data is required by Applicable Privacy Laws.

2.1.6.1. Semaphore Consulting shall provide evidence of the deletion, removal or return of the Personal Data.

3. Sub-processing

3.1. Customer provides its general authorisation for Semaphore Consulting to appoint subprocessors.

3.2. Semaphore Consulting shall inform the Customer of any intended changes concerning the addition or replacement of a Subprocessor prior to such changes, thereby giving the Customer the opportunity to object to such changes. The objection shall be made by written communication within 10 business days after receiving notice of a new Subprocessor. Semaphore Consulting shall use reasonable efforts to replace the Subprocessor. If Semaphore Consulting is unable to locate a Subprocessor that will be amenable to the Customer, Semaphore Consulting shall request a revision to the License Conditions to exclude the processing activities related to the work that the Subprocessor was going to perform.

3.3. The Customer has the right to ask Semaphore Consulting to replace the Subprocessor for cause. If Semaphore Consulting cannot remedy the issue, replace the Subprocessor or assume the obligations of the Subprocessor, the Customer has the right to terminate this Agreement and the License Conditions for cause.

3.4. A list of approved Subprocessors included in Schedule 1 shall be maintained by the Processor to ensure that it is up-to-date and current. Semaphore Consulting will not share any Personal Data with any other party outside of those listed in Schedule 1.

3.5. Semaphore Consulting shall enter into written agreements with each subprocessor that contains terms substantially the same as those which are outlined within this DPA.

3.6. If the Subprocessor fails to comply with the Agreement, the Applicable Privacy Laws or any other applicable national and/or local legislation, Semaphore Consulting shall remain fully liable to the Customer.

4. Security of Processing

4.1. Semaphore Consulting shall implement and maintain technical or organisational measures (and has received assurances that all Subprocessors have implemented and maintained technical and organisational measures) to identify and investigate Personal Data breaches.

4.2. Without undue delay and within 48 of hours notify the Customer of becoming aware of any data breach, whether reportable or otherwise. Semaphore Consulting shall provide all information as the Customer requires to report the circumstances to the relevant regulator(s)/ Data Protection Supervisory Authorities and to notify affected Data Subjects under Applicable Privacy Laws, including:

4.2.1. Description of the breach, including, if possible, the categories of data and records concerned, the category and number of Data Subjects affected;

4.2.2. Likely consequences of the breach;

4.2.3. Measures taken or proposed to address and/or mitigate the effects of the breach;

4.2.4. Name and contact of the Data Protection Officer or any contact point where further information can be reached.

4.3. The Data Protection Officers from both Parties shall cooperate to comply with the obligation to notify the Data Protection Authorities and Data Subjects in accordance with all requirements in Applicable Privacy Laws. Semaphore Consulting shall comply with all requests for assistance made by the Customer.

4.4. Semaphore Consulting shall, without undue delay, take all urgent measures and cooperate with the Customer's breach response protocol to contain the Data Breach and protect the Personal Data.

5. Audit

5.1. Semaphore Consulting shall make available to the Customer documentation regarding its compliance with this Agreement and Applicable Privacy Laws.

5.2. Upon prior notice and no more than once a year, the Customer has the right to conduct an audit to verify compliance with the Agreement.

5.2.1. Notwithstanding the previous provision, the Customer has the right to conduct more than one (1) yearly audit in case of a Data Breach.

5.2.2. The Customer shall schedule the audit with Semaphore Consulting at least 2 weeks in advance.

Both Parties shall agree upon the scope, the timing, and the duration of the audit.

5.3. The audit might be carried out by the Customer directly or by a third-party auditor appointed by the Customer.

5.4. Semaphore Consulting has the right to object to the use of a particular third-party auditor, if it could be considered a competitor.

Schedule 1

Details of Processing

1. Nature and Purpose of Processing

The Processor will process Personal Data on behalf of the Controller for the purpose of report generation. This processing is necessary for the performance of the services outlined in the main agreement between the parties.

2. Categories of Data Subjects

The Personal Data processed concerns the following categories of data subjects:

- Teachers
- Students
- Parents

3. Types of Personal Data

The Personal Data processed includes, the following categories:

Teachers: Full name, email address, gender

Students: Full name, email address, age, gender, home group, grades, class enrolments

Parents: Full name, email address, relationship to students

4. Special Categories of Personal Data (if applicable)

The Processor will process the following special categories of data only as when required by the Customer and in compliance with applicable data protection laws:

Customer may choose to process special categories of data within Accelerus, including student medical data.

5. Duration of Processing

Processing will continue for the duration of the License Conditions between the parties, unless otherwise required by law or specifically agreed.

7. Security Measures

The Processor shall implement appropriate technical and organisational measures to ensure the security of Personal Data, including but not limited to:

- Access controls and authentication
- Data encryption
- Regular security assessments
- Secure data storage and transmission
- Employee training on data protection

Semaphore Consulting's full list of technical security measures can be reviewed at upon request.

8. Sub-Processors

The Processor may engage the following sub-processors in the provision of its services:

Entity Name	Sub-processing Activity	Processing Location(s)
Microsoft Azure	Hosting, Data Storage	UK, Australia
SendGrid	Send emails	United States

9. International Data Transfers

Where Customer chooses cloud-hosting provided by Accelerus (.com.au domain) and is located outside of Australia, Personal Data will be transferred to Australia. The Processor shall ensure adequate safeguards are in place, such as an International Data Transfer Agreement (UK) or EU Standard Contractual Clauses (SCCs).