Data Processing Addendum

This Data Processing Addendum, dated as of ("***Addendum***"), by and between (the "***Controller***"), and **SHOWBIE Inc. DBA Showbie**, a Canadian corporation (the "***Service Provider***") (collectively referred to as the ***"Parties"***), sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by the Service Provider to the Controller pursuant to Showbie's Terms of Use and the order submitted by the Controller for the Services (together, the "***Master Agreement***").

Whereas, the Controller or its employees, agents, consultants or contractors (collectively, "***Controller Personnel***") shall provide the Service Provider with access to Personal Data in connection with certain services performed by the Service Provider for or on behalf of the Controller pursuant to the Master Agreement; and

Whereas, the Controller requires that the Service Provider preserve and maintain the privacy, confidentiality, and security of such Personal Data.

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Master Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, the Controller and Service Provider agree as follows:

I. Definitions

(A) ***"Applicable Law"*** means all applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive"), as replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications.

(B) "***Data Controller***" has the meaning set out in the Applicable Law.

(C) "***Data Processor***" has the meaning set out in the Applicable Law.

(D) ***"Data Security Measures"*** means technical and organisational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorised access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.

(E) ***"Data Subject"*** means an identified or identifiable natural person to whom the Personal Data pertains.

(F) "**Instructions**" means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

(G) "**Notification Related Costs**" means the Controller's and its affiliates' internal and external costs associated with investigating, addressing and responding to a Personal Data Breach, including but not limited to: (i) preparation and mailing or other transmission of any notifications or other communications to customers, potential customers, clients, employees, agents or others as Controller deems reasonably appropriate; (ii) establishment of a call center or other communications procedures in response to such Personal Data Breach (e.g., customer service FAQs, talking points and training); (iii) public relations and other similar crisis management services; (iv) legal, accounting, consulting and forensic expert fees and expenses associated with the Controller's and its affiliates' investigation of and response to such Personal Data Breach; and (v) costs for commercially reasonable credit monitoring, identity protection services or similar services that Controller determines are advisable under the circumstances.

(H) "**Personal Data**" means any information relating to an identified or identifiable natural person Processed by the Service Provider in accordance with the Controller's Instructions pursuant to this Addendum; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(I) "**Personal Data Breach**" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

(J) "**Process**", "**Processed**", or "**Processing**" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(K) "**Sub-Processor**" means the entity engaged by the Data Processor or any further Sub- Processor to Process Personal Data on behalf and under the authority of the Data Controller.

II. Roles and Responsibilities of the Parties

(A) The Parties acknowledge and agree that the Controller is acting as a Data Controller and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data under this Addendum, and the Service Provider is acting as a Data Processor on behalf and under the Instructions of the Controller.

(B) Any Personal Data will at all times be and remain the sole property of the Controller and the Service Provider will not have or obtain any rights therein.

III. Obligation of the Service Provider

The Service Provider agrees and warrants to:

(A) Process Personal Data disclosed to it by the Controller only on behalf of and in accordance with the Instructions of the Controller and Annex 1 of this Addendum, unless the Service Provider is otherwise required by Applicable Law, in which case the Service Provider shall inform the Controller of that legal requirement before Processing the Personal Data, unless informing the Controller is prohibited by law on important grounds of public interest. The Service Provider shall immediately inform the Controller if, in the Service Provider's opinion, an Instruction provided infringes Applicable Law.

(B) Hold in strict confidence (i) the existence and terms of the Master Agreement (including this Addendum), and any related agreement, and (ii) any and all Personal Data.

(C) Ensure that any person authorised by the Service Provider to process Personal Data in the context of the Services is only granted access to the Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Controller.

(D) Not transfer Personal Data outside the country from which the Controller or its Personnel originally delivered to the Service Provider, or from which the Service Provider otherwise accessed or obtained such Personal Data or, if it was originally delivered to a location inside the European Economic Area ("EEA") or Switzerland, outside the EEA or Switzerland, for Processing without the explicit written consent of the Controller (where such consent is deemed to have been granted in respect of the jurisdictions listed in Annex 1) and only in compliance with Applicable Laws. The Service Provider shall enter into any written agreements as are necessary (in the Controller's reasonable determination) to comply with Applicable Law concerning any cross-border transfer of Personal Data, whether to or from the Service Provider. If, in the performance of the Master Agreement, Processor transfers any Personal Data received from or on behalf of Controller to any third party (which shall include without limitation any affiliates of Processor) where such third party is located outside the European Economic Area, Processor shall ensure:

a) that the third party execute Standard Contractual Clauses for transfers from Data Controllers to Data Processors approved by the Commission pursuant to Decision 2010/87/EU, as amended by Commission Implementing Decision (EU) 2016/2297;
b) the third party to be certified under the Privacy Shield framework; or
c) the existence of any other specifically approved safeguard for data transfers (as recognized under the GDPR) and/or a European Commission finding of adequacy.

For greater certainty, the Standard Contractual Clauses will be employed for any transfer of Personal Data by the Processor or any of its sub-processors to South America, Asia, or Australia.

(E) Inform the Controller promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing, as well as their right to data portability, and not respond to such requests, unless instructed by the Controller in writing to do so. Taking into account the nature of the Processing of Personal Data, the Service Provider shall assist the Controller, by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.

(F) Notify the Controller immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. The Controller shall have the right to defend such action in lieu of and on behalf of the Service Provider. The Controller may, if it so chooses, seek a protective order. The Service Provider shall reasonably cooperate with the Controller in such defense.

(G) Provide reasonable assistance to the Controller in complying with the Controller's obligations under Applicable Law.

(H) Maintain internal record(s) of Processing activities, copies of which shall be provided by the Service Provider to the Controller or supervisory authorities upon request. Such records must contain at least: (i) the name and contact details of the Service Provider; (ii) the categories of Processing activities carried out under this Addendum; (iii) information on data transfers to a third country or a third party, where applicable; and (iv) a general description of the Data Security Measures implemented to protect Personal Data processed under this Addendum.

IV. Sub-Processing

(A) The Service Provider shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless the Controller has authorised the Service Provider to do so in writing. Where the Service Provider, with the consent of the Controller, provides access to Personal Data to a third party, the Service Provider shall enter into a written agreement with each such third party that imposes obligations on the third party that are the same as those imposed on the Service Provider under this Addendum. The Service Provider shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data.

(B) Where that other processor fails to fulfil its data protection obligations, the Service Provider shall remain fully liable to the Controller for the performance of that other processor's obligations.

V. Compliance with Applicable Laws

(A) The Service Provider shall comply with all Applicable Laws.

(B) The Service Provider represents and warrants that no Applicable Law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim prohibits the Service Provider from fulfilling its obligations under this Addendum.

(C) The Service Provider shall in good faith negotiate any further Data Processing Agreement reasonably requested by the Controller for purposes of compliance with the Applicable Law. In case of any conflict between this Addendum and the Master Agreement, this Addendum shall prevail with regard to the Processing of Personal Data covered by it.

VI. Data Security

(A) The Service Provider shall develop, maintain, and implement a comprehensive written information security program that complies with Applicable Law including, but not limited to, the Data Security Measures described in Annex 2 of this Addendum. The Service Provider's information security program shall include appropriate administrative, technical, physical, organisational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

a) The pseudonymization and encryption of the 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 the 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 technical and organisational measures adopted pursuant to this provision for ensuring the security of the Processing.

(B) The Service Provider shall supervise Service Provider Personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. The Service Provider shall provide training, as appropriate, regarding the privacy, confidentiality and information security requirements set forth in this Addendum to all Service Provider Personnel who have access to Personal Data.

(C) Promptly upon the expiration or earlier termination of the Master Agreement, or such earlier time as the Controller requests, the Service Provider shall return to the Controller or its designee, or at the Controller's request, securely destroy or render unreadable or indecipherable if return is not reasonably feasible or desirable to the Controller (which decision shall be based solely on the Controller's written statement), each and every original and copy in every media of all Personal Data in the Service Provider's, its affiliates' or their respective subcontractors' possession, custody or control. Promptly following any return or alternate action taken to comply with this Clause VI(C), the Service Provider shall provide to the Controller a completed certificate certifying that such return or alternate action occurred. In the event applicable law does not permit the Service Provider to comply with the delivery or destruction of the Personal Data, the Service Provider warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.

VII. Data Breach Notification

(A) The Service Provider shall immediately inform the Controller in writing of any Personal Data Breach of which the Service Provider becomes aware, but in no case longer than twenty four (24) hours after it becomes aware of the Personal Data Breach. The notification to the Controller shall include all available information regarding such Personal Data Breach, including information on:

a) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;
b) The likely consequences of the Personal Data Breach; and
c) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Service Provider shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with the Controller in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. The Service Provider shall provide such assistance as required to enable the Controller to satisfy the Controller's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR. The content of any filings, communications, notices, press releases or reports related to any

Personal Data Breach must be approved by the Controller prior to any publication or communication thereof. The Service Provider shall be responsible for the costs and expenses associated with the performance of its obligations described in this paragraph, unless the Personal Data Breach is caused by the acts or omissions of the Controller or its affiliates.

(B) In the event of a Personal Data Breach involving Personal Data in the Service Provider's possession, custody or control or for which the Service Provider is otherwise responsible, the Service Provider shall reimburse the Controller on demand for all commercially reasonable Notification Related Costs incurred by the Controller arising out of or in connection with any such Personal Data Breach.

VIII. Audit

Service Provider shall on written request (but not more than once per year, other than in the event of a breach) make available to the Controller all information necessary to demonstrate compliance with the obligations set forth in this Addendum and, at the Controller's expense, allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Upon prior written request by the Controller (provided that it shall be not more than once per year other than in the event of a breach), the Service Provider agrees to cooperate and, within reasonable time, provide the Controller with: (a) audit reports and all information necessary to demonstrate Service Provider's compliance with the obligations laid down in this Addendum; and (b) confirmation that the audit has not revealed any material vulnerability in the Service Provider's systems, or to the extent that any such vulnerability was detected, that the Service Provider has fully remedied such vulnerability. The Service Provider's failure to comply with this obligation shall entitle the Controller to suspend the Processing of Personal Data Processed by the Service Provider, and to terminate any further Processing of Personal Data, this Addendum and/or the Master Agreement, if doing so is required to comply with Applicable Law.

IX. Injunctive Relief

The Service Provider agrees that any Processing of Personal Data in violation of this Addendum, the Controller's Instructions or any Applicable Law, or the occurrence of any Personal Data Breach, will cause immediate and irreparable harm to the Controller for which money damages will not constitute an adequate remedy. Therefore, the Service Provider agrees that the Controller may seek and be granted specific performance and injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages.

X. Liability

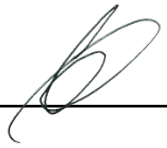
The Service Provider agrees to indemnify and hold the Controller harmless from and against any direct damages, fines, costs or expenses that it may incur or that arise out of or in connection with a third party claim relating to any violation of this Addendum.

IX. Governing Law

To the extent required by Applicable Law, this Addendum shall be governed by the law of **Ireland.** In all other cases, this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

IN WITNESS WHEREOF, the parties acknowledge their agreement to the foregoing by due execution of the Addendum by their respective authorised representatives.

Showbie

Signature: 

Name: Colin Bramm

Title: CEO and Cofounder

Address: #403, 10113 104 Street, Edmonton, AB Canada T5J 1A1

Phone: 1.866.925.3904

Date: May 1, 2018

Signature:

Name:

Title:

Address:

Phone:

Date:

ANNEX 1: SCOPE OF THE DATA PROCESSING

SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between the Controller and the Service Provider.

The Processing of Personal Data concerns the following categories of Data Subjects:

1) Teachers and administrators
2) Students
3) Parents

The Processing concerns the following categories of Personal Data:

1) User's login information and usage within the Service
2) User profile information
3) Student assignments, grades, interactions and messaging

The Processing concerns the following categories of Sensitive Data:

Sensitive Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation.

Status as a student at a religious school, if applicable.

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):

1) Purpose of processing Customer user login and platform solely to provide the services.
2) Purpose of managing Student assignments, grades and progress.

The duration of data processing is the duration of the contract.

The Service Provider uses the following Sub-Processors:
Showbie data sub-processors

The Service Provider may transfer and process personal information to and in the following jurisdictions outside of the EU:
Canada
United States
South America
Asia
Australia

ANNEX 2: DATA SECURITY MEASURES

This Annex forms part of the Data Processing Addendum between the Controller and the Service Provider. Taking into account the state of the art, the costs of implementation and the nature, scope, content and purpose of the Processing, the Service Provider agrees to implement the following Data Security Measures:

1. Physical access control

Technical and organisational measures to prevent unauthorised persons from gaining access to the data Processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are Processed, including:

- Establishing security areas, restriction of access paths;
- Establishing access authorisations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralised data Processing equipment and personal computers.

2. Logical access control

Technical and organisational measures to prevent data Processing systems from being used by unauthorised persons, including:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and temporary turn-off of the user ID upon ten erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data Processing environment;
- Encryption and pseudonymisation.

3. Data access control

Technical and organisational measures to ensure that persons entitled to use a data Processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorisation, including:

- Internal policies and procedures;
- Control authorisation schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;

- Disciplinary action against employees who access personal data without authorisation;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption and pseudonymisation.

4. Disclosure control

Technical and organisational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Logging;
- Transport security;
- Encryption and pseudonymisation.

5. Entry control

Technical and organisational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data Processing systems, including:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of Instructions

Technical and organisational measures to ensure that Personal Data are Processed solely in accordance with the Instructions of the Controller, including:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organisational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Backup procedures;
- Mirroring of hard disks;
- Uninterruptable power supply;
- Remote storage;
- Strong firewall systems;
- Continual security updates;
- Disaster recovery plan.

8. Separation control

Technical and organisational measures to ensure that Personal Data collected for different purposes can be Processed separately, including:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.