Appendix 1: Data Processing Agreement

1. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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;

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Data Protection Legislation" means any law, statute, directive, or regulation, including any and all legislative and/or regulatory amendments or successors thereto, regarding privacy, data protection, information security obligations and/or the processing of Personal Data (including, but not limited to, 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 processing of personal data and the free movement of that data ("GDPR"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations ("CCPA"), the Children's Online Privacy Protection Act of 1998 ("COPPA")), the New York State Education Law Section 2-D relating to Unauthorized Release of Personally Identifiable Information ("2D") and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted.

"Personal Data Breach" means an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data that is Processed.

Any capitalized terms used in this Agreement that have not been defined herein shall have the same meaning given to them in the Data Protection Legislation.

2. General information

This Data Processing Agreement sets out the terms and conditions under which the Supplier Processes the Customer's Personal Data. The objective of this Data Processing Agreement is to take into account the responsibilities and obligations between the Contracting Parties as set out in the Data Protection Legislation.

Concerning the Personal Data Processed in connection with the service provided by the Supplier, the Customer is the data controller, who defines the purposes and means for the Processing of Personal Data, or a processor of Personal Data or a service provider, who Processes Personal Data on behalf of a third party. The Supplier is a data processor or a service provider, who Processes the Personal Data on behalf of the Customer and based on an assignment received from the Customer in accordance with the terms and conditions set out in this Appendix. In Appendix 1.1, the Contracting Parties agree, at a more detailed level, on the types of data subjects, the processing measures taken by the Supplier, data protection procedures and the purposes for which the Supplier Processes the Customer's Personal Data.

The Contracting Parties understand that authorities may issue orders and instructions relating to the scope of application of the Data Protection Legislation after the signing of the Agreement and undertake to supplement this Data Protection Agreement as required based on such orders and instructions.

Each Contracting Party provides the other Contracting Party with the contact details of their data protection officers or, in case no data protection officer has been appointed, the contact details of the person responsible for compliance with Data Protection Legislation.

3. Responsibilities of the Customer

The Customer Processes Personal Data in accordance with the Data Protection Legislation. The Customer is responsible for ensuring that the instructions concerning the Processing of Personal Data, included as Appendix 1.2, are lawful, complete and correct. Any amendments to the instructions in Appendix 1.2 and the cost effect of such changes are always agreed upon separately in writing.

The Customer is responsible for the Personal Data delivered to the Supplier and for the lawfulness of the Processing for the entire duration of the Agreement. The Customer is responsible for ensuring that all data subjects whose Personal Data is being processed have been provided with the required notifications and information relating to the Processing of Personal Data, as set out in Data Protection Legislation. The Supplier is not monitoring the content, quality or up-to-dateness of the Personal Data that is delivered.

The Customer is responsible for ensuring that the purpose and grounds for the Processing of Personal Data comply with the Data Protection Legislation. This includes ensuring that Personal Data is collected in accordance with the Data Protection Legislation and that the Customer has the right to transfer the Personal Data to the Supplier for Processing.

4. Responsibilities of the Supplier

The Supplier Processes Personal Data in accordance with the Data Protection Legislation and the written instructions set out in Appendix 1.2, unless the Data Protection Legislation applicable to the Supplier requires otherwise. In this case, the Supplier notifies the Customer of such legislative requirements before the Processing, unless prohibited from doing so under the Data Protection Legislation. For the sake of clarity, it is stated that the Customer is always deemed to have instructed the Supplier to provide the services related to the Processing of Personal Data as set out in the Agreement.

Taking into account the nature of the Processing activities, the Supplier assists the Customer, by using appropriate technical and organizational measures of the Supplier's choosing, to fulfil the Customer's obligation to respond to requests concerning the exercising of the following rights of data subjects, as set out in the Data Protection Legislation (provided that the data subject has the right in question under the Data Protection Legislation):

a) right to access Personal Data;
b) right to the rectification and erasure of Personal Data;
c) right to restriction of processing;
d) right to Personal Data portability; and
e) right to object to the processing of Personal Data.

If actions are required from the other Contracting Party in order to fulfil the request, each Contracting Party notifies the other Contracting Party of any requests concerning the exercising of the rights of data subjects as soon as possible after receiving such a request. When notifying the other party, the Contracting Party must provide all information required for the fulfilment of the request. If the fulfilment of a request requires an unreasonable amount of work from the Supplier, the Supplier has the right to charge for such work separately in accordance with the price list valid at the given time.

Taking into account the nature of the Processing activities and the information available to the Supplier, the Supplier assists the customer to comply with the following obligations set out in Data Protection Legislation:

a) ensuring the security of the Processing of Personal Data through appropriate technical and organizational measures:
b) notifying the applicable governmental authorities and data subjects of any Personal Data Breaches;
c) participating, as necessary, to any data protection impact assessments if such an assessment is required under Data Protection Legislation; and
d) participating, as necessary, to any prior consultation if such a consultation is required under Data Protection Legislation.

The Supplier is obligated to assist the Customer only within the scope of the obligations imposed on the data processor or a service provider under the Data Protection Legislation. If the provision of assistance requires an unreasonable amount of work from the Supplier, the Supplier has the right to charge an hourly fee for such work separately in accordance with the price list valid at the given time.

5. CCPA Specific Supplier Obligations

The Supplier acknowledges and agrees that:

1) The Supplier is acting solely as a Service Provider with respect to Personal Information;

2) The Supplier shall not (1) Sell Personal Information, or (2) retain, use or disclose Personal Information (i) for any purpose other than for the specific purpose of performing the services set out in the Agreement, or (ii) outside of the direct business relationship between the Supplier and the Customer;

3) Upon the Customer's request, the Supplier shall promptly delete a particular individual's Personal Information from the Supplier's records. In the event the Supplier is unable to delete the Personal Information for reasons permitted under the CCPA, the Supplier shall (i) promptly inform the Customer of the reason(s) for its refusal of the deletion request, (ii) ensure the privacy, confidentiality and security of such Personal Information, and (iii) delete the Personal Information promptly after the reason(s) for the Supplier's refusal has expired;

4) The Personal Information that the Customer discloses to the Supplier is provided to the Supplier for a Business Purpose, and the Customer does not Sell Personal Information to the Supplier in connection with the Agreement; and

5) The Supplier certifies that it understands and will comply with the requirements and restrictions set forth in this Section 5.

6. Information Security

The Contracting Parties undertake to agree and implement technical and organizational measures commonly used in the industry in order to protect Personal Data from accidental and unlawful processing and disclosure. When the Contracting Parties agree on the implementation of such measures, the following must be taken into account in planning and implementation: the state of the art technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. When evaluating the appropriate security level, the Contracting Parties must also consider the risks related to the Processing, especially unauthorized and unlawful Processing of Personal data and any accidental loss, destruction or damage.

Such measures include, for example,

a) the pseudonymization 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 technical and organizational measures for ensuring the security of the Processing.

The above-mentioned measures are examples of how the Contracting Parties can ensure the security of the Processing of Personal Data. The Contracting Parties agree, in Appendix 1.1, on the above-mentioned measures and other information security-related procedures that the Supplier takes concerning the Processing of Personal Data. The Customer is responsible for ensuring appropriate and adequate information security concerning the equipment and operational information technology environment that the Customer is responsible for. Unless otherwise agreed in the Agreement, the Customer is responsible for taking back-ups of Personal Data and for checking that the back-ups are functioning.

The Customer is responsible for notifying the Supplier of any issues related to the Personal Data delivered by the Customer, such as risk evaluations and Processing related to special or sensitive categories of Personal Data, which affect the technical and organizational measures implemented in accordance with this Data Processing Agreement. For the sake of clarity, it is stated that any amendments to the information security procedures agreed in Appendix 1.2 and the cost effect of such changes are always agreed upon separately in writing.

The Supplier ensures that the persons who Process Personal Data have undertaken to comply with non-disclosure obligations or that they are bound by appropriate statutory non-disclosure obligations. The Supplier takes the required measures to ensure that the persons in question Process the Personal Data only in accordance with the instructions set out in Appendix 1.2.

7. Subcontractors

The list of current subcontractors for the service provision and the related Processing of Personal Data is attached hereto as Appendix 1.3. The Supplier has no right to use additional subcontractors without the prior written consent of the Customer, which shall not be unreasonably withheld or denied. The Supplier is responsible for ensuring that subcontractors process Personal Data in accordance with this Data Processing Agreement and the Data Protection Legislation.

The Supplier will notify the Customer if it plans to change or add any subcontractors participating in the Processing of Personal Data. The Customer has the right to object to such changes based on reasonable grounds. The Customer must submit a notification of such an objection without undue delay after receiving information from the Supplier concerning the matter. If the Customer does not approve the change or addition concerning a subcontractor, the Supplier has the right to terminate the Agreement with a notice period of thirty (30) days.

8. Personal Data Breaches

Each Contracting Party notifies the other Contracting Party, without undue delay and not later than within 36 hours, of any Personal Data Breaches it becomes aware of. In connection with the notification concerning a Personal Data Breach, the Customer must provide the Supplier with all information that can be deemed to help investigate, limit or prevent the Personal Data Breach. The Contracting Parties may agree on the notification process separately at a more detailed level. Unless agreed otherwise by the Contracting Parties, the notification must be submitted to the contact person appointed by the Contracting Party.

In connection with submitting the notification of a Personal Data Breach, the Supplier must provide the Customer with the following:

a) a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number

of personal data records concerned (in so far as the information in question is available to the Supplier);

b) the name and contact details of the Supplier's data protection officer or other contact point where more information can be obtained;
c) a description of the likely consequences of the Personal Data Breach; and
d) a description of the measures taken by the Supplier to address the Personal Data Breach, including any measures taken by the Supplier to mitigate the possible adverse effects of the Personal Data Breach.

If the Personal Data Breach is attributable to reasons for which the Customer is responsible, the Customer is liable for any costs incurred by the Supplier as a result of the Personal Data Breach. The Customer is responsible for notifying the governmental authorities and data subjects of any Personal Data Breaches in accordance with the provisions set out in the Data Protection Legislation.

9. Records of Processing Activities

The Supplier maintains a record of the Processing activities that it carries out on behalf of the Customer. The record contains the following information:

a) the name and contact details of the Customer, Supplier and their data protection officers and information on any subcontractors;
b) Processing activities carried out on behalf of the Customer; and
c) where possible, a general description of the technical and organizational security measures specified in section 5.

10. Right to Audit

During the Agreement period, the Customer or an independent expert appointed by the Customer, who cannot be a competitor of the Supplier, has the right to verify that the Supplier complies with the obligations imposed on the Supplier under this Agreement. The object of the audit includes the Supplier's materials relevant to the Processing of Personal Data and the Supplier's systems and premises used for the Processing of Personal Data. The Supplier must be notified of such an audit in writing at least thirty (30) days in advance. Notwithstanding the above, the Supplier must always allow all audits of the operations of data processors carried out by the authorities supervising the operations of the Customer. This Data Processing Agreement is applied, where applicable, to any audits carried out by authorities.

The Supplier participates in the audit and provides the Customer with all information that is required to verify that the Supplier complies with the obligations imposed on the Supplier under this Data Processing Agreement. The audit may not hinder the service production of the Supplier, and the auditors have no right to access the information of the Supplier's customers or cooperation partners. If the audit is carried out by some other party than the Customer, the auditor and Supplier conclude a non-disclosure agreement before the audit is performed.

The Customer is liable for all costs incurred as a result of the audit and compensates the Supplier for the costs that the Supplier incurs as a result of the audits. If significant defects in the Supplier's operations are discovered through the audits, the Supplier is liable for its own costs it incurs as a result of the audits.

11. Termination of the Processing of Personal Data

The Supplier erases Personal Data when the Agreement terminates, and the services related to the Processing of Personal Data cease to be provided. The Customer may obligate the Supplier to return the Personal Data to the Customer by submitting a written request. In addition, the Supplier erases all existing copies of the Personal Data at the termination of the Agreement, unless the Supplier is required to retain the Personal Data in question based on legislation or an order issued by authorities. The Supplier has the

right to charge the Customer an hourly fee for the returning or erasing of Personal Data in accordance with the Supplier's price list valid at the given time. The Contracting Parties may agree in more detail on the practices concerning the erasing and returning of Personal Data.

12. Consent

IF YOU ARE AN AUTHORIZED SCHOOL ADMINISTRATOR OR STAFF, YOU PROVIDE YOUR CONSENT TO USE OF THE SERVICES ON BEHALF OF A CHILD AND REGISTRATION WITH THE SERVICES AS DESCRIBED IN THE AGREEMENT, AND YOU AGREE TO THE PROVISIONS OF THIS DATA PROCESSING AGREEMENT WITH RESPECT TO USE OF THE SERVICES AS DESCRIBED IN THE AGREEMENT WITH RESPECT TO A GIVEN STUDENT/CHILD. YOU FURTHER WARRANT AND REPRESENT THAT PARENTAL CONSENTS HAVE BEEN OBTAINED IN COMPLIANCE WITH COPPA AND/AS REQUIRED, OTHER DATA PROTECTION LEGISLATION.

13. Damage Incurred as a Result of the Processing of Personal Data

If a data subject suffers damage as a result of an infringement of the Data Protection Legislation, each Contracting Party itself is liable for any damage incurred by a data subject in accordance with the Data Protection Legislation. In addition, each Contracting Party itself is liable for any administrative fines imposed on it by the governmental authorities.

The provisions set out in the Agreement concerning the limitation of liability are applied to this Data Processing Agreement.

13. Appendices

Appendix 1.1 Description of the processed personal data
Appendix 1.2 Instructions on the processing of personal data

Appendix 1.3 List of sub-contractors

Appendix 1.1: Description of the Processed Personal Data

The Contracting Parties may supplement and amend this Appendix as necessary.

1. Purpose of the Processing of Personal Data

The Supplier processes the Personal Data only in accordance with the agreements concluded with the customer in order to provide software services offered by the Supplier.

2. Content of the Processing

The Supplier carries out the following Processing activities concerning Personal Data:

Collection	Consultation
Recording	Use
Organization	Making information available (disclosure, for example, by transmission or dissemination)
Structuring	Alignment or combination
Storage	Restriction
Adaptation or alteration	Erasure or destruction
Retrieval	
Other processing activities, please specify:	

3. Categories of Data Subjects and Personal Data Records Subject to Processing

The Supplier Processes the following categories of data subjects and personal data records:

Category of data subjects	Personal data	Special or sensitive categories of personal data
Students	Name, email address, name of the school, class level	
Students, Staff	Username	
Staff	Name, email address, classes and class levels taught	

Students, Staff	Answers to questions submitted in the service	

4. Applicable Data Protection Procedures

The Supplier adheres to its own internal data protection instructions when Processing Personal Data. In addition, the Supplier implements the following data protection measures:

- Material that is processed electronically is collected into databases that are protected by firewalls, passwords and other technical means, and access rights to the databases are restricted and granted only to persons whose work duties require them to use the systems.
- A username and password are required for system use, and only persons authorized to carry out the tasks can access the personal data that is processed.
- The data connection from the user's browser to the Supplier's server is encrypted.

Appendix 1.2: Instructions on the Processing of Personal Data

As a part of the Service, the Customer will transfer Personal Data to the Supplier's servers. The parties state that, in this case, the Supplier Processes the Personal data on behalf of the Customer, with the Customer being the data controller that determines the purposes and means of Processing.

In so far as anonymous aggregate data and other data that cannot be linked to individual persons is created as a result of this Processing, the Supplier has the right to utilize the generated non-personal data for the purpose of developing the Service and the related tools without a separate consent of the parties.

The Supplier emphasizes and the Customer accepts that the Supplier does not create back-up copies of the Personal Data the Customer uploads to the Service. The Customer is solely responsible for the maintenance of the data.

Appendix 1.3.

LIST OF SUBCONTRACTORS

Microsoft Ltd.

School Day uses Microsoft Azure as the service and data platform.