

**STANDARD STUDENT DATA PRIVACY
AGREEMENT**

CA-NDPA Standard
Version 1.0 (10.22.20)

And

Class Technologies, Inc.

August 18, 2021

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

(the "**Local Education Agency**" or "**LEA**") and Class _____, located at

Technologies, Inc. (the "**Provider**" or "**Class**"). _____, located at

WHEREAS, the Provider is providing educational or digital services, specifically a SaaS based virtual classroom designed for use with Zoom to LEA.

WHEREAS, the Provider and LEA recognize the need to _____ protect personally identifiable student information (PII, as defined in Exhibit C) and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99);

the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations

and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions. Check if Required**

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby

_____ incorporated by reference into this DPA in their entirety.

_____ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: _____ Title: _____

Address: _____

Phone: _____ Email: _____

The designated representative for the Provider for this DPA is:

Name: Tess Frazier Title: SVP & Chief Compliance Officer

Address: 1717 N. St. NW Suite 1 Washington DC 20036

Phone: _____ Email: legal@class.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA:

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

PROVIDER:

By: _____ Date: _____

Printed Name: Tess Frazier Title/Position: SVP & Chief Compliance Officer

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to

the Class Order Form and Class Subscription License and Service Agreement (“Service Agreement”), Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account. Intentionally omitted.**

4. **Law Enforcement Requests.** Should law enforcement or other government entities {"Requesting Party(ies)"} contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA {34 CFR § 99.31{a}{l}}, LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A and/or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted in writing by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified

Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de- identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after sixty (60) days. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** At the LEA's expense and no more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity Framework utilizing elements set forth in **Exhibit "H"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "H"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a Data Breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Data Breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Data Breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**, be bound by the terms of **Exhibit "E"** to any other Subscribing LEA who signs the acceptance on said Exhibit, as well as the Class Order Form, including the Class Subscription License and Services Agreement. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent SO long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H (which contains terms specific to the Vednro and Agreement), the SDPC Standard Clauses, and/or the Supplemental State Terms (found at Exhibit G and which contains state terms that differ from the SDPC standard clasues), Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.]

Train the Trainer

Class Technologies professional services team will train your trainers. We will provide 4 hrs. of learning and development delivered as a series of webinars.

Managed Implementation

SSO configuration; LTI configuration courses; SIS data export mapping; Premium setup and onboarding - custom branding

Class for Zoom Annual License (up to 5000 students)

IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT
(RESOURCE) HERE]

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System		
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X		
	Other application technology meta data- Please specify:			
Application Use Statistics	Meta data on user interaction with application	X		
Assessment	Standardized test scores			
	Observation data			
	Other assessment data-Please specify: Quiz assessment data results	X		
Attendance	Student school (daily) attendance data			
	Student class attendance data	X		
Communications	Online communications captured (emails, blog entries)	X		
Conduct	Conduct or behavioral data			
Demographics	Date of Birth			
	Place of Birth			
	Gender			
	Ethnicity or race			
	Language information (native, or primary language spoken by student)			
	Other demographic information-Please specify:			
Enrollment	Student school enrollment			
	Student grade level			
	Homeroom			
	Guidance counselor			
	Specific curriculum programs			
	Year of graduation			
	Other enrollment information-Please specify: class-level enrollment, pulled from the LMS. An in-class roster can be created by the instructor	X		
Parent/Guardian Contact Information	Address			
	Email			
	Phone			

Category of Data	Elements	Check if Used by Your System		
Parent/Guardian ID	Parent ID number (created to link parents to students)			
Parent / Guardian Name	First and/or Last			
Schedule	Student scheduled courses	X		
	Teacher names	X		
Special Indicator	English language learner information			
	Low income status			
	Medical alerts/ health data			
	Student disability information		<input type="checkbox"/>	
	Specialized education services (IEP or 504)			
	Living situations (homeless/foster care)			
	Other indicator information-Please specify:			
Student Contact Information	Address			
	Email	X		
	Phone			
Student Identifiers	Local (School district) ID number			
	State ID number			
	Provider/App assigned student ID number			
	Student app username			
	Student app passwords			
Student Name	First and/or Last	X		
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)		<input type="checkbox"/>	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in		<input type="checkbox"/>	
Student Survey Responses	Student responses to surveys or questionnaires	X		
Student work	Student generated content; writing, pictures, etc.			
	Other student work data -Please specify: poll, quiz, and assignment submissions	X		
Transcript	Student course grades			
	Student course data			
	Student course grades/ performance scores			

Category of Data	Elements	Check if Used by YOU! System		
	Other transcript data - Please specify:			
Transportation	Student bus assignment			
	Student pick up and/or drop off location			
	Student bus card ID number			
	Other transportation data - Please specify:			
Other	Please list each additional data element used, stored, or collected by your application:			

None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable .	<input type="checkbox"/>
------	--	--------------------------

EXHIBIT C:
DEFINITION

Data Breach: means the unauthorized release, acquisition, access, destruction, or loss of computerized data, including personal information. A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of a Data Breach to the LEA and/or the student (1) whose unencrypted personal information was, or is reasonably believed to have been, subject to a Data Breach; or (2) whose encrypted personal information was, or is reasonably believed to have been, subject to a Data Breach, and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person, and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without reasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the Data Breach and restore the reasonable integrity of the data system.

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: A local education agency who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order and/or Terms of Service and/or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

I 190353v1

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

1190353v1

EXHIBIT "D"
**DIRECTIVE FOR DISPOSITION OF
DATA**

Provider to dispose of data obtained by Provider

pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

1 190353v1

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and

("Originating LEA") which is dated _____, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below and resulting Class Order Form including the Class Subscription License and Services Agreement. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

PROVIDER: Class Technologies, Inc. _____

BY: _____ Date: _____

Printed Name: Tess Frazier Title/Position: SVP & Chief Compliance Officer

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the

and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

LEA: _____

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology - Security techniques - Information security management systems (ISO 27000 series)

<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.eds.pex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Supplemental SDPC State Terms for California
Version 1.0

This Amendment for Student Data Privacy Consortium ("SDPC") State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

, located at (the "**Local Education Agency**" or "**LEA**") and
, located at
(the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

Term. The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.

Modification to Article IV, Section 7 of the DPA. Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

[SIGNATURES BELOW]

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA:

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

PROVIDER:

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

EXHIBIT "H" **Vendor Specific Terms**

INFORMATION SECURITY POLICY

Purpose

Protecting the confidentiality, integrity and availability of customer information, records and transactions is critical to Class. Class considers all customer information confidential, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. All Class staff share in the responsibility to our clients and customers, to ensure that the appropriate procedures and controls are implemented and that information security remains a constant priority.

This policy is not designed to act as a substitute for sound risk analysis or good judgment. The primary objective of the policy is to ensure the appropriate protection of Class customer information, records and transactions handled by computer and data communication systems owned by or administered for Class.

Policy Statement

All information collected, processed, stored on or transmitted over Class computer systems and networks will be treated as a Class corporate asset. It is the policy of Class to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of our sensitive information assets. Class will maintain an information security program to control risks associated with access, use, storage, sharing, and destruction of sensitive customer and financial information. This program will document minimum standards of behavior for staff, contractors and service providers and include clear guidance for the day-to-day operations of Class. At a minimum, the program must include:

- Risk Assessment
- Risk Mitigation and Management
- Monitoring and Reporting
- Audit
- IT Oversight and Program Adjustment
- Vendor Management

Standards for Risk Assessment

Each critical process deployed at Class will undergo a comprehensive risk assessment to identify critical information assets, threats to those assets, and effectiveness of risk controls. The risk assessment will review risks to the entire process and not limited to specific IT systems. The risk assessment will be updated on an annual basis. The Information Security Officer (ISO), Peter Dudka, in conjunction with the Leadership Team, must decide to what degree potential losses will be mitigated to reduce risk to Class, staff, partners and members. For each system, service, or activity offered by or through Class, the company will conduct a risk assessment.

As threats, operating environment (physical and virtual) and systems architecture change, the ISO in conjunction with the Chief Compliance Officer and Leadership Team, will update the risk assessment to ensure new risks are mitigated before making changes to infrastructure, policies or procedures. At a minimum, the Leadership Team and BOD will review the comprehensive risk assessment at least once per year.

Standards for Risk Management and Security Control Measures

All information systems require effective and reliable controls to maintain data confidentiality, assure availability and integrity, ensure customer privacy, and protect Class computer and telecommunications systems from unauthorized intrusions and access, misuse, or fraud. Based upon justification detailed in the risk assessment, Class will implement controls that support the following principles.

POLICY DEVELOPMENT

A critical part of our risk mitigation plan is to provide policies and risk mitigation guidelines to our staff and partners. We will leverage best practices to develop policies and document security procedures to meet operational risk mitigation objectives as well as compliance with customer privacy expectations and other regulatory requirements.

ACCESS CONTROLS

All Class computers and telecommunications systems will limit access to users who have a proven "need-to-know". Access to confidential information must be granted on a minimum level of access necessary to perform assigned responsibilities and will be monitored for compliance pursuant to the Access Control Policy.

PHYSICAL SECURITY

Critical, confidential, and sensitive client/ member information and information processing systems must be physically protected from unauthorized access, damage and service disruption. Such protection will be in accordance with the Physical Security Policy and the Information Classification Policy.

ENCRYPTION

Any system or service requiring the transmission or storage of information such as social security numbers (SSN's), passwords, non-public personal financial information including credit reporting information, account numbers, and payment card data will use an approved method of encryption as a means of protecting data. Approved encryption methods will be defined and determined by the Class ISO. Any transmission of sensitive company information and/or non-public personal staff or customer information sent via email must be encrypted and / or password protected. Additional protection will be in accordance with the Cryptography Controls Policy and the Information Classification Policy.

SYSTEMS DEVELOPMENT LIFE CYCLE

Class considers all servers, workstations, network devices, security systems, peripheral equipment, data and application software as valuable company assets. In order to mitigate its exposure to risk, we have established policies and set standards for the acquisition, installation and maintenance of all hardware and software in the Systems Development Lifecycle (SDLC) Policy.

CHANGE MANAGEMENT

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Class will establish formal management responsibilities and procedures to ensure satisfactory control of all changes to equipment, software and procedures. Operational programs will be subject to strict change control. The details of change and configuration management are outlined in the Change Management Policy.

CONFIGURATION MANAGEMENT

The IT Systems and Network Operations Policy outlines minimum configuration requirements required to deploy a system. Hardening guidelines will be created based on the minimum requirements established by the policy. Antivirus must be installed on all systems before being allowed on the network.

PERSONNEL SECURITY

Human threats represent the one of most significant hazards to safe and secure delivery of our services. To mitigate hazards introduced by our staff, Class will enforce safeguards contained in our Personnel Security Policy. At a minimum, that policy will address hiring and termination procedures to grant authorized access to company systems and data along with provisions for training. All new employees will receive security training as a part of new employee orientation. All employees will receive annual security training on a schedule determined by company management. This training will include a review of relevant IT Policies, technology changes, and the procedures to follow in maintaining the confidentiality of classified data.

MONITORING SYSTEMS

The Information Security Officer will supervise regular monitoring of the critical systems in use by Class and evaluate whether the controls are functioning effectively and that no security breaches have occurred. At a minimum, standards established in the Security Operations Policies will address the following:

1. Exception reports for security policy violations will be immediately reported to the Leadership Team;
2. Summary reports of all event log analysis will be provided to the Leadership Team at least once per quarter;
3. Vulnerability assessments, penetration tests and other events and access monitoring will be periodically performed using approved security tools to verify vulnerabilities are mitigated within 30 days of receiving vulnerability notices and security policies and procedures are enforced. Results will be analyzed and policies/controls modified as needed to prevent, detect and respond to possible security breaches.

INFORMATION SECURITY INCIDENT RESPONSE

Information security incident response is an important component of our information technology program. Appropriate responses to information security incidents are defined in the Incident Response Policy.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The continuation of our services after a disaster or service disruption is critical to the success of Class. A Business Continuity Plan (BCP) with integrated Disaster Recovery Plan will be maintained by the Information Security Officer in accordance with our Business Continuity Policy. Company management will participate in developing the plans, training staff and conducting annual tests to ensure the organization, its staff and clients are protected from anticipated hazards.

PERIMETER SECURITY

Class will maintain the security controls to protect company assets and information as justified by the risk assessment. Perimeter security controls are specified in the IT Systems and Network Operations Policy will include the following safeguards:

1. Firewall(s)
2. Intrusion Detection System (IDS)
3. Virus Protection
4. Router Management

TRAINING

Training is an important part of ensuring the confidentiality, integrity and availability for customer and company information. In order to minimize possible security risks, all company staff will be trained in their specific responsibilities under the information security program.

Standards for Service Provider Oversight

A periodic review of all mission-critical outsourcing arrangements will be performed to confirm that Class service providers and critical vendors comply with the Vendor Management Policy defined in this document. Class has integrated critical business partners into the delivery of services to customers. Therefore, each service provider who has access to sensitive company systems or information must comply with the guidelines for selection, contracting and monitoring as specified in the vendor management policy and associated procedures. It is the responsibility of the process owner to present new or changed requirements to service providers to the Leadership Team for approval.

**STANDARD STUDENT DATA PRIVACY
AGREEMENT**

CA-NDPA Standard
Version 1.0 (10.22.20)

And

Class Technologies, Inc.

August 18, 2021

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between: Irving Unified School District (the "Local Education Agency" or "LEA"),

located at 6050 Barranca Pkwy, Irvine, CA 92604

and Class Technologies, Inc. (the "Provider" or "Class"),

located at 1717 N Street, NW, Suite #1, Washington, DC. 20036 USA

WHEREAS, the Provider is providing educational or digital services, specifically a SaaS based virtual classroom designed for use with Zoom to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information (PII, as defined in Exhibit C) and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions. Check if Required**

If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby

incorporated by reference into this DPA in their entirety.

If checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Michelle Bennett Title: IT CONTRACTS SPECIALIST
Address: 6050 Barranca Pkwy, Irvine, CA 92604
Phone: _____ Email: Michelle.Bennett@iUSD.org

The designated representative for the Provider for this DPA is:

Name: Tess Frazier Title: SVP & Chief Compliance Officer
Address: 1717 N. St, NW Suite 1 Washington DC 20036
Phone: _____ Email: legal@class.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: IRVINE UNIFIED SCHOOL DISTRICT

By: _____ Date: August 18, 2021
Printed Name: John Fogarty Title/Position: ASST. Supt BUSINESS SERVICES
iUSD Board Approved 8/17/2021

PROVIDER: Class Technologies, Inc.

By: Tess Frazier Date: 8/5/2021
DocuSigned by: 02002993294E100...

Printed Name: Tess Frazier Title/Position: SVP & Chief Compliance Officer

STANDARD CLAUSES
Version 3.0

ARTICLE I: PURPOSE AND SCOPE

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict,

definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Class Order Form and Class Subscription License and Service Agreement ("Service Agreement"), Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account. Intentionally omitted.**

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA {34 CFR § 99.31(a)(l)}, LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A and/or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted in writing by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified

Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de- identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after sixty (60) days. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Article II section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** At the LEA's expense and no more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity Framework utilizing elements set forth in **Exhibit "H"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "H"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a Data Breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Data Breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a Data Breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**, be bound by the terms of **Exhibit "E"** to any other Subscribing LEA who signs the acceptance on said Exhibit, as well as the Class Order Form, including the Class Subscription License and Services Agreement. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H (which contains terms specific to the Vendor and Agreement), the SDPC Standard Clauses, and/or the Supplemental State Terms (found at Exhibit G and which contains state terms that differ from the SDPC standard clauses), Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.]

Train the Trainer

Class Technologies professional services team will train your trainers. We will provide 4 hrs. of learning and development delivered as a series of webinars.

Managed Implementation

SSO configuration; LTI configuration courses; SIS data export mapping; Premium setup and onboarding - custom branding

Class for Zoom Annual License (up to 5000 students)

IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT (RESOURCE) HERE]

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Observation data	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Other assessment data-Please specify: Quiz assessment data results	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Student class attendance data	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Place of Birth	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Gender	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Student grade level	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Homeroom	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Year of graduation	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Other enrollment information-Please specify: class-level enrollment, pulled from the LMS. An in-class roster can be created by the instructor	X <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Email	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Phone	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System		
Parent/Guardian ID	Parent ID number (created to link parents to students)			
Parent / Guardian Name	First and/or Last			
Schedule	Student scheduled courses	X		
	Teacher names	X		
Special Indicator	English language learner information			
	Low income status			
	Medical alerts/ health data			
	Student disability information		<input type="checkbox"/>	
	Specialized education services (IEP or 504)			
	Living situations (homeless/foster care)			
	Other indicator information-Please specify:			
Student Contact Information	Address			
	Email	X		
	Phone			
Student Identifiers	Local (School district) ID number			
	State ID number			
	Provider/App assigned student ID number			
	Student app username			
	Student app passwords			
Student Name	First and/or Last	X		
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)		<input type="checkbox"/>	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in		<input type="checkbox"/>	
Student Survey Responses	Student responses to surveys or questionnaires	X		
Student work	Student generated content; writing, pictures, etc.			
	Other student work data -Please specify: poll, quiz, and assignment submissions	X		
Transcript	Student course grades			
	Student course data			
	Student course grades/ performance scores			

Category of Data	Elements	Check if Used by Your System		
	Other transcript data - Please specify:			
Transportation	Student bus assignment			
	Student pick up and/or drop off location			
	Student bus card ID number			
	Other transportation data - Please specify:			
Other	Please list each additional data element used, stored, or collected by your application:			

None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable .	<input type="checkbox"/>
------	--	--------------------------

EXHIBIT C:
DEFINITION

Data Breach: means the unauthorized release, acquisition, access, destruction, or loss of computerized data, including personal information. A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of a Data Breach to the LEA and/or the student (1) whose unencrypted personal information was, or is reasonably believed to have been, subject to a Data Breach; or (2) whose encrypted personal information was, or is reasonably believed to have been, subject to a Data Breach, and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person, and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without reasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the Data Breach and restore the reasonable integrity of the data system.

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: A local education agency who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order and/or Terms of Service and/or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

I 190353v1

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

1190353v1

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF
DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

DocuSigned by:
Traci Frasier

8206283294E486
Authorized Representative of Company

8/5/2021

Date

I 190353v1

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology - Security techniques - Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)

<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit [http:// www.eds pex.org](http://www.eds.pex.org) for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Supplemental SDPC State Terms for California
Version 1.0

This Amendment for Student Data Privacy Consortium ("SDPC") State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between: IRVINE USD (the "**Local Education Agency**" or "**LEA**") , located at 6000 BAYVIEW PI and Class Technologies, Inc. (the "**Provider**") located at 1717 N Street, NW, Suite #1, Washington, DC. 20036 USA. All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

Term. The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.

Modification to Article IV, Section 7 of the DPA. Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

[SIGNATURES BELOW]

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Irving Unified School District

By:  _____

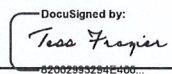
Date: August 18, 2021

Printed Name: John Fogarty

Title/Position: ASST Supt BUSINESS SERVICES

USD Board Approval 8/17/2021

PROVIDER:

By:  _____
DocuSigned by:
Tess Frazier
62002985294E100...

Date: 8/5/2021

Printed Name: Tess Frazier

Title/Position: SVP & CCO

EXHIBIT "H" **Vendor Specific Terms**

INFORMATION SECURITY POLICY

Purpose

Protecting the confidentiality, integrity and availability of customer information, records and transactions is critical to Class. Class considers all customer information confidential, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. All Class staff share in the responsibility to our clients and customers, to ensure that the appropriate procedures and controls are implemented and that information security remains a constant priority.

This policy is not designed to act as a substitute for sound risk analysis or good judgment. The primary objective of the policy is to ensure the appropriate protection of Class customer information, records and transactions handled by computer and data communication systems owned by or administered for Class.

Policy Statement

All information collected, processed, stored on or transmitted over Class computer systems and networks will be treated as a Class corporate asset. It is the policy of Class to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of our sensitive information assets. Class will maintain an information security program to control risks associated with access, use, storage, sharing, and destruction of sensitive customer and financial information. This program will document minimum standards of behavior for staff, contractors and service providers and include clear guidance for the day-to-day operations of Class. At a minimum, the program must include:

- Risk Assessment
- Risk Mitigation and Management
- Monitoring and Reporting
- Audit
- IT Oversight and Program Adjustment
- Vendor Management

Standards for Risk Assessment

Each critical process deployed at Class will undergo a comprehensive risk assessment to identify critical information assets, threats to those assets, and effectiveness of risk controls. The risk assessment will review risks to the entire process and not limited to specific IT systems. The risk assessment will be updated on an annual basis. The Information Security Officer (ISO), Peter Dudka, in conjunction with the Leadership Team, must decide to what degree potential losses will be mitigated to reduce risk to Class, staff, partners and members. For each system, service, or activity offered by or through Class, the company will conduct a risk assessment.

As threats, operating environment (physical and virtual) and systems architecture change, the ISO in conjunction with the Chief Compliance Officer and Leadership Team, will update the risk assessment to ensure new risks are mitigated before making changes to infrastructure, policies or procedures. At a minimum, the Leadership Team and BOD will review the comprehensive risk assessment at least once per year.

Standards for Risk Management and Security Control Measures

All information systems require effective and reliable controls to maintain data confidentiality, assure availability and integrity, ensure customer privacy, and protect Class computer and telecommunications systems from unauthorized intrusions and access, misuse, or fraud. Based upon justification detailed in the risk assessment, Class will implement controls that support the following principles.

POLICY DEVELOPMENT

A critical part of our risk mitigation plan is to provide policies and risk mitigation guidelines to our staff and partners. We will leverage best practices to develop policies and document security procedures to meet operational risk mitigation objectives as well as compliance with customer privacy expectations and other regulatory requirements.

ACCESS CONTROLS

All Class computers and telecommunications systems will limit access to users who have a proven "need-to-know". Access to confidential information must be granted on a minimum level of access necessary to perform assigned responsibilities and will be monitored for compliance pursuant to the Access Control Policy.

PHYSICAL SECURITY

Critical, confidential, and sensitive client/ member information and information processing systems must be physically protected from unauthorized access, damage and service disruption. Such protection will be in accordance with the Physical Security Policy and the Information Classification Policy.

ENCRYPTION

Any system or service requiring the transmission or storage of information such as social security numbers (SSN's), passwords, non-public personal financial information including credit reporting information, account numbers, and payment card data will use an approved method of encryption as a means of protecting data. Approved encryption methods will be defined and determined by the Class ISO. Any transmission of sensitive company information and/or non-public personal staff or customer information sent via email must be encrypted and / or password protected. Additional protection will be in accordance with the Cryptography Controls Policy and the Information Classification Policy.

SYSTEMS DEVELOPMENT LIFE CYCLE

Class considers all servers, workstations, network devices, security systems, peripheral equipment, data and application software as valuable company assets. In order to mitigate its exposure to risk, we have established policies and set standards for the acquisition, installation and maintenance of all hardware and software in the Systems Development Lifecycle (SDLC) Policy.

CHANGE MANAGEMENT

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Class will establish formal management responsibilities and procedures to ensure satisfactory control of all changes to equipment, software and procedures. Operational programs will be subject to strict change control. The details of change and configuration management are outlined in the Change Management Policy.

CONFIGURATION MANAGEMENT

The IT Systems and Network Operations Policy outlines minimum configuration requirements required to deploy a system. Hardening guidelines will be created based on the minimum requirements established by the policy. Antivirus must be installed on all systems before being allowed on the network.

PERSONNEL SECURITY

Human threats represent the one of most significant hazards to safe and secure delivery of our services. To mitigate hazards introduced by our staff, Class will enforce safeguards contained in our Personnel Security Policy. At a minimum, that policy will address hiring and termination procedures to grant authorized access to company systems and data along with provisions for training. All new employees will receive security training as a part of new employee orientation. All employees will receive annual security training on a schedule determined by company management. This training will include a review of relevant IT Policies, technology changes, and the procedures to follow in maintaining the confidentiality of classified data.

MONITORING SYSTEMS

The Information Security Officer will supervise regular monitoring of the critical systems in use by Class and evaluate whether the controls are functioning effectively and that no security breaches have occurred. At a minimum, standards established in the Security Operations Policies will address the following:

1. Exception reports for security policy violations will be immediately reported to the Leadership Team;
2. Summary reports of all event log analysis will be provided to the Leadership Team at least once per quarter;
3. Vulnerability assessments, penetration tests and other events and access monitoring will be periodically performed using approved security tools to verify vulnerabilities are mitigated within 30 days of receiving vulnerability notices and security policies and procedures are enforced. Results will be analyzed and policies/controls modified as needed to prevent, detect and respond to possible security breaches.

INFORMATION SECURITY INCIDENT RESPONSE

Information security incident response is an important component of our information technology program. Appropriate responses to information security incidents are defined in the Incident Response Policy.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The continuation of our services after a disaster or service disruption is critical to the success of Class. A Business Continuity Plan (BCP) with integrated Disaster Recovery Plan will be maintained by the Information Security Officer in accordance with our Business Continuity Policy. Company management will participate in developing the plans, training staff and conducting annual tests to ensure the organization, its staff and clients are protected from anticipated hazards.

PERIMETER SECURITY

Class will maintain the security controls to protect company assets and information as justified by the risk assessment. Perimeter security controls are specified in the IT Systems and Network Operations Policy will include the following safeguards:

1. Firewall(s)
2. Intrusion Detection System (IDS)
3. Virus Protection
4. Router Management

TRAINING

Training is an important part of ensuring the confidentiality, integrity and availability for customer and company information. In order to minimize possible security risks, all company staff will be trained in their specific responsibilities under the information security program.

Standards for Service Provider Oversight

A periodic review of all mission-critical outsourcing arrangements will be performed to confirm that Class service providers and critical vendors comply with the Vendor Management Policy defined in this document. Class has integrated critical business partners into the delivery of services to customers. Therefore, each service provider who has access to sensitive company systems or information must comply with the guidelines for selection, contracting and monitoring as specified in the vendor management policy and associated procedures. It is the responsibility of the process owner to present new or changed requirements to service providers to the Leadership Team for approval.