

EVERFI, Inc. and the Perris Union High School District
Memorandum of Understanding

This **MEMORANDUM OF UNDERSTANDING** (the “**Agreement**”) is made and entered into as of the **19th** day of **August, 2022** (the “**Effective Date**”), by and between **EVERFI, Inc.** (“EVERFI”) and the **Perris Union High School District**, on behalf of itself and each of its participating schools (collectively, “District”). For purposes of this Agreement, EVERFI and the District shall be referred to individually as a “Party” and collectively as the “Parties”.

WHEREAS, EVERFI is a leading education technology company with the mission to help Districts teach critical topics such as financial capability, character education, career choice and digital literacy; and

WHEREAS, the District wants to empower students to succeed in school, college, careers and life and believes that EVERFI’s digital curriculum will help teachers provide engaging, high quality, and consistent instruction to do so; and

WHEREAS, EVERFI and the District desire to create an agreement to bring EVERFI curriculum to schools within the District.

NOW, THEREFORE, for good consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties, intending to be legally bound, agree as follows:

Responsibilities of EVERFI:

EVERFI shall:

- Provide EverFi's sponsored digital curriculum to schools within the District at no cost. This curriculum will be available the entire school year and in the summer, and the specific resources and objectives can be found at www.EVERFI.com/k12.
- Provide free educator training. EVERFI can deliver educator training sessions on an individual teacher/school basis or large group basis. Large group training sessions are preferred.
- Provide real-time data for teachers on student progress via a digital teacher dashboard.
- Provide timely support to teachers regarding implementation or technical questions related to its digital curriculum.
- Provide an annual Impact Report to the District highlighting the impact of the curriculum.
- Provide opportunities for schools, as available, to interact with program sponsors, including special events, classroom visits, and other opportunities.
- Include District teachers and administrators in webinars and other events hosted by EVERFI about life skills for students.
- Provide the District with marketing materials to promote the program and its impact, including press releases, social media guides, and more.
- Meet high standards for student data privacy – EVERFI’s K12 policy is outlined in Exhibit A.
- Provide the District with an EVERFI point of contact for the program and for any contract related questions.

- Provide access to EVERFI's curriculum through the District's SSO provider.

Responsibilities of the District:

The District shall:

- Identify an overall point person for EVERFI to coordinate an annual meeting and other partnership details.
- Identify additional points of contact, for each subject area, who can help determine the appropriate placement for EVERFI sponsored learning courses. The placement of the courses will aim to reach the most students and achieve the best student outcomes.
- Invite EVERFI staff to present at relevant teacher PD's throughout the school year or help set up other means of training teachers.
- Meet with EVERFI staff annually over the summer to review the results of the annual Impact Report and to discuss the partnership for the following school year.
- Complete an annual survey providing feedback to EVERFI staff about the partnership.
- As District deems appropriate, share elements of the partnership via social media and other outlets or provide a thank you or recognition to the sponsors funding EVERFI's programs.
- Ensure that EVERFI has teacher and student SIS information for all relevant grades and subject areas prior to the beginning of each school year. This information will be used by EVERFI to provide teachers and students access to the EVERFI curriculum through the district's single-sign-on. See exhibit B for EVERFI's full K12 data sharing agreement.

Term:

This Agreement is for the entire school year and will renew automatically each year on July 1st for the upcoming and academic year through June 30, 2027 (5 year Agreement). Both EVERFI and the District also reserve the right to terminate this Agreement upon thirty (30) days prior written notice if the other Party fails to perform the terms and conditions in this Agreement.

Mutual Protections:

This Agreement shall be interpreted and governed by the laws of the state of California, excluding any laws that direct the application of another jurisdiction's law.

Except as required by law, neither Party shall be liable to the other for consequential, special, punitive, incidental or indirect damages whether arising in contract, in tort or otherwise in connection with performance or failure to perform the Agreement.

In the event that any provision or provisions of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall continue in full force and effect.

Any modification or assignment of the Agreement will be effective only if in writing and signed by both parties. A waiver of any term or condition of this Agreement must be in writing executed by both parties.

Any notices to be given under this Agreement by either party to the other may be effected by personal delivery in writing or by mail, registered or certified, postage prepaid with return receipt requested.

This Agreement may be executed in any number of counterparts.

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the date and year first above written.

EVERFI, INC.

Signed: 

Print: Jessica Golden

Title: _Senior Director, K12

Date: July 15, 2022

DISTRICT Perris Union High School District

Signed: _____

Print: _____

Title: _____

Date: _____

EXHIBIT A

EVERFI K12 Data Privacy Policy

Overview

As a provider of online content, EVERFI takes student privacy very seriously and complies with two specific pieces of legislation protecting student privacy:

- **Family Education Rights and Privacy Act (FERPA):** Mandated by the Department of Education to protect the privacy of education records while still allowing for effective use of data.
- **Children's Online Privacy Protection Act (COPPA):** Mandated by the FTC to protect children under 13 from unfair or deceptive uses of personal information.

Both of these regulations address third party handling of Personally Identifiable Information (PII) and Education Records. EVERFI collects a narrow set of PII, referred to as "Directory Information" under FERPA. Schools have the right to share this information with EVERFI, and EVERFI has the right to store this information so long as the information is not disclosed to third parties, and there are proper measures in place to delete all records upon request.

As a practice, EVERFI only uses PII for core business practices such as troubleshooting technical issues and presenting teachers with reports for individual students (such as rosters and scores). All student data, when analyzed internally or shared externally, is aggregated and de-identified, meaning it cannot be traced back to individual students.

PII Related Data Being Stored (K-12)

- Date of Birth is shared via SSO integration (to support COPPA compliance) but is only stored as an over/under 13 flag within EVERFI's system.
- If a student is flagged as over 13, email is stored if included in data share, and first name and last name are required.
- If a student is flagged as under 13, email is not collected and first name and first initial of last name (1 character only) is required for the sole purpose of helping teachers identify students.

General Privacy Policy and Data Security

EVERFI DOES NOT:

- Use student data to create student profiles or perform any other type of data mining that might result in damaging or discriminatory representations of student ability
- Use or sell student data for commercial purposes, such as creating targeted ads
- Use or sell student data for marketing research purposes
- Share email addresses or individual student data with third parties
- Store PII data on removable drives
- Email PII data directly to anyone

EVERFI DOES:

- Analyze and report on student data in de-identifiable and/or aggregate form, either to improve our learning products or communicate the impact of a program to third parties. Data is retained only for educational purposes.
- Use best of breed cloud-based hosting and system admin services in Amazon Web Services to host and keep all data secure
- Encrypt all data at rest, encrypt all hard-drives, and use TLS encryption for data transfer
- Use role-based access control on a need-to-know basis for staff
- Incorporate appropriate password policies based on specific roles and markets
- Archive and remove student data every 4 years (on a rolling basis)
- Run vulnerability and penetration security testing
- Have formal policies and programs in place regarding:
 - System Change Management
 - Staff Security Training and Review
 - System Log Monitoring, Review, and Audit
 - User Access Monitoring, Review, and Audit
 - Service Interruption Contingency and Support Escalation

Exhibit B EVERFI K12 Data Sharing Agreement

Description of Data to be provided upon written consent to the following conditions and restrictions, the District will provide the following digital data, as requested, to EVERFI through Clever:

1st-12th Grade Teachers: First Name, Last Name, Email, Subject, School, Section, Grade, Clever ID, Sections
1st - 12th Grade Students: First Name, Last Name or Last Initial, Email (optional), School, Birth date, Clever ID

Terms of Agreement

Data provided by the District is subject to the following conditions and restrictions:

A. Subject Data Layers Conditions and Restrictions:

1. Digital layers provided by the District are solely for the original recipient's internal use in the conduct of its educational affairs.
2. No digital layers may be reproduced or redistributed without the District prior written permission.
3. Access to the digital data provided by the District shall be exclusively for the contractor/volunteer and employees only. The term 'employee' shall mean any person directly employed on a full-time or part-time basis by the District. The term 'employee' shall also be construed to mean any contractor, consultant or any similar person or entity hired by the District for a limited purpose.
4. The District shall require any third party contractor hired to perform work that utilizes digital data to agree not to use, reproduce, or redistribute the District data for any purpose other than indicated by prior agreement. All copies of District data used by a third party contractor must be returned to District upon contract work completion. The provisions of this paragraph apply in equal force to any independent contractor the District employee or approved volunteer shall provide any third party contractor with a copy of this signed agreement and the District representative shall approve data exchange.

B. Liabilities and Limitations for the Accuracy of Digital Data Provided:

1. By signing this Agreement, The User shall become contractually bound to all provisions stated in this Agreement.
2. Although the District has verified the digital data to the best of its ability, the District makes no representations of any kind as to its complete accuracy; nor does it guarantee the complete accuracy of any digital data furnished. The District additionally makes no warranties of merchantability or fitness for a particular use, nor is such warranties to be implied, with respect to the digital data provided under this Agreement.
3. The User is responsible for understanding the accuracy limitations of all digital data provided. In particular, alterations and/or manipulation of the original data may adversely affect their accuracy, meaning, and design integrity.
4. The User agrees to hold the District and all its employees, and agents harmless from any claim, suit, or proceeding arising out of the use of the data in accordance with this agreement, including indemnification of the District for reasonable expenses incurred in defending such claims.

C. Production of Printed Map/Report/Publication Products Using Digital Data Provided:

1. The User may not reproduce digital data layers in the form of a printed product provided while assuming duties as stated.
2. Any maps, reports, or publications created using the digital data provided by the District shall give credit to the District by using the following statement/disclaimer:
"This (map/report/publication/data) was created using the District's Information Systems digital data, but this is a secondary product which has not been verified or authorized by District"

D. Sharing of the District Data with Other Persons or Entities:

If at any time during the course of this Agreement, The User determines that it is necessary to share portions of the District data with a person or entity not employed by the District as a consultant, contractor, or any similar person or entity for a limited public purpose, The User shall first request permission from the District before sharing any portion of the District data, unless otherwise committed by this Agreement or as required by law. Any such request shall be in writing to the

District and shall specify the persons or entities The User wishes to share the District data with and the reasons why such sharing of information is necessary. Permission for The User to share the District data provided by the District with other parties shall not be unreasonably withheld if such sharing of information is necessary to further legitimate legal purposes. Commercial or revenue-generating uses of the District data shall not be considered a legitimate purpose.

The undersigned hereby accepts and agrees to be bound by the terms and conditions set forth in the Data Sharing Agreement. It is fully understood that pursuant to this agreement the undersigned is permitted to utilize digital information provided by the District, solely in the conduct of its own educational business affairs. Any other use unless with prior written permission from the District shall be deemed unauthorized.

The District makes no representations of any kind, including but not limited to the warranties of merchantability or fitness for a particular use, nor are any such warranties to be implied, with respect to the digital data furnished hereunder.

The District assumes no responsibility to maintain them in any manner or form.

STANDARD STUDENT DATA PRIVACY AGREEMENT

**CA-NDPA Standard
Version 1.0 (10.25.20)**

and

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:

_____, located at _____
(the “**Local Education Agency**” or “**LEA**”) and _____, located at _____
(the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

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 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: _____ Title: _____

Address: _____

Phone: _____ Email: _____

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: _____ Title/Position: _____

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 Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 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.
- 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.
- Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

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)(1)), 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 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 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 providing the LEA with reasonable prior notice. 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 section II 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**. 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 based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. 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 "F"**. 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 LEA who signs the acceptance on said Exhibit. 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, the SDPC Standard Clauses, and/or the Supplemental State Terms, 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

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.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
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:	
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	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	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	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
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.	

EXHIBIT "C" DEFINITIONS

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: An LEA 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 or Terms of Service 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,

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."

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

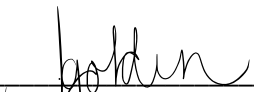
EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

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. 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: _____

BY:  _____ Date: _____

Printed Name: _____ Title/Position: _____

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)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	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.edspex.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 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:

1. **Term**. The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.
2. **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: Golden _____ Date: _____

Printed Name: _____ Title/Position: _____