CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

IRVINE UNIFIED SCHOOL DISTRICT

and

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA, UNIVERSITY OF CALIFORNIA SAN DIEGO

May 9, 2021

This California Student Data Privacy Agreement ("DPA") is entered into by and between the IRVINE UNIFIED SCHOOL DISTRICT (hereinafter referred to as "LEA") and THE REGENTS OF THE UNIVERSITY OF CALIFORNIA,ON BEHALF OF ITS SAN DIEGO CAMPUS (hereinafter referred to as "Provider") on May 9, 2021. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Local Education Agency ("LEA") wishes to use certain Provider digital educational services ("Services"), described below in Article I(2) and Exhibit "A", and

WHEREAS, in order to provide the Services, the Provider may receive and the LEA may provide documents or data that are covered by several Federal and State statutes, among them, the Federal Educational and Privacy rights Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

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 transmitted to Provider from the LEA in order to provide the Services, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing these Services, the Provider shall be considered a School Official with a legitimate educational interest performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA for purposes of providing Services that require collecting, maintaining, or using Personally Identifiable Information ("PII") from LEA's students. Control duties are set forth below.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

The CSU/UC Mathematics Diagnostic Testing Project (MDTP) develops and provides free diagnostic tools and training to support California mathematics educators in preparing students for success in current and subsequent mathematics courses. MDTP offers these free services through our online testing platforms or through traditional paper testing and scoring.

3. **Student Data to Be Provided**. In order for Provider to perform the Services, LEA shall provide the categories of data attached hereto as Exhibit "B".

4. **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 privacy or use terms that either party has publicized.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider for purposes of the Services is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records processed for purposes of providing Services 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 LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer Pupil Generated Content to a separate account, according to the procedures set forth below.

2. **Parent Access**. Provider and the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of Pupil Generated Content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the LEA's request for personally identifiable information in a Pupil's Records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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**. Provider shall, at the request of the LEA, transfer Pupil Generated Content, as defined by AB 1584, to a separate student account.

4. **Third Party Request**. Except where required by law or regulation, Provider shall redirect any Third Party requesting LEA data held by the Provider pursuant to the Services to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than to provide Services described in Article I(2) above.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors who handle LEA-provided Student PII related to the Services, whereby the Subprocessors agree to be bound by the relevant terms of this DPA, provided, however, that if these terms are in conflict with the terms of a Subcontractor contract in effect before execution of this DPA, this provision shall not apply to that agreement until the expiration, amendment, or renewal of that agreement.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Services in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA. LEA shall list or substantially describe Provider or Provider Services in its FERPA or privacy notice as an authorized recipient of Student Data.

2. **Data Minimization and Use Limitation**. LEA shall provide Provider no more PII than is required for provision of Services or as otherwise stated in this DPA. LEA shall only use data and results provided by Provider in compliance with the Service acceptable use and privacy terms.

3. **Reasonable Precautions**. LEA is responsible for designating users who have an authorized purpose for accessing the Service and data, providing and revoking such access, and implementing administrative policies and safeguards to prevent inappropriate access, use, or disclosure of Service and data. LEA shall designate users and grant access in compliance with FERPA and teacher or employee contracts. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access or use of Service, data, usernames, or passwords. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

5. **District Representative**. At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

6. **Restriction on Use of Results for Teacher Evaluations.** LEA agrees that Services and diagnostic results are provided to LEA solely for purposes of assessing and enhancing student readiness. In no event will LEA use Services, results, or data collected via MDTP for purposes of evaluating, assessing, or disciplining teachers or other employees or affiliates.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including but not limited to FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Authorized Use**. The Student Data shared for the Services, including persistent unique identifiers, shall be used for no purpose other than the Services and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared for the Services. Provider agrees to inform each employee or agent with access to Student Data of the confidentiality obligations of this DPA and the administrative sanctions in case of non-compliance.

4. **No Disclosure**. Provider shall not disclose any data obtained through the Service in a manner that could identify an individual student to any other entity. Deidentified information may be used by the Provider and its Subprocessors for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data**. Upon termination, provider shall dispose of or transfer all personally identifiable Student Data obtained through the Service to LEA or LEA's designee according to a schedule and procedure as the Parties may reasonably agree. If Student Data is to be disposed of, upon request, provider shall provide written notification to LEA when the Data has been disposed. If disposal or transfer is infeasible, Provider shall continue to extend all security and privacy protections of this DPA to the PII for the duration of its maintenance and refrain from using or disclosing Student Data. Nothing authorizes Provider to maintain personally identifiable data obtained for purposes of providing Services beyond the time period reasonably needed to complete the disposition or as required by law. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Parties agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access.** Provider shall make reasonable efforts to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data by:

      Using secure user authentication protocols including: i. Control of user IDs and other identifiers; ii. A secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; iii. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; iv. Restricting access to active users and active user accounts only; and v. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. vi. Periodic review of user access, access rights and audit of user accounts.

      Using secure access control measures that: i. Restrict access to records and files containing PII and systems to those who need such information to perform their job duties; and ii. Assign unique identifications plus passwords to each person with computer access, which are reasonably designed to maintain the integrity of the security of the access controls.

   b. **Security Protocols.** Both parties agree to maintain security protocols in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated for purposes of the Services in a secure computer environment and not copy, reproduce, or transmit such data, except as necessary for backups of data to ensure availability or to fulfill the purpose of data requests by LEA.

   c. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

   d. **Security Technology.** The service shall use a secure cryptographic protocol (TLS v. 1.2 or higher), or equivalent technology to protect data from unauthorized access. The service security measures shall include server authentication and data; encryption of all transmitted records and files containing PII; adequate security of all networks that connect to the system or access PII, including wireless networks; reasonable monitoring of systems, for unauthorized use of or access to PII and system resources; encryption of all PII stored on devices, including laptops or other portable storage devices; for files containing PII on a system that is connected to the Internet, reasonably up-to-date firewall, router and switch protection and operating system security patches, reasonably designed to maintain the integrity of the PII; reasonably up-to-date versions of system security agent software, including intrusion detection systems, which must include

malware protection and reasonably up-to-date patches and virus definitions. Provider shall host Student Data in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Upon request, provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data.

2. Data Breach.

Incidents. In the event of suspected or actual unauthorized access, use, or disclosure of Student Data, the Parties agree to cooperate to mitigate and investigate the incident. Decisions related to obligations of breach notification to the Students or regulators shall be made in good faith and based on the level of control over the breached mechanism and connection with the affected data subjects.

Breaches and Reporting. In accordance with Cal. Civ. Code §1798.29, in the event of a breach of the security of the system or the Service that includes unencrypted Student Data and such Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the breach. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall employ the following or similar titles and headings: titled "Notice of Data Breach," "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

   i. The name and contact information of the reporting Provider 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.

   v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.

e. At the request and with the assistance of the LEA, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY 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 this DPA 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. Term. Both Parties shall be bound by this DPA for the duration of LEA's use of Services or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, the Parties agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. Termination. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent. Either Party may terminate this agreement unilaterally by providing notice pursuant to Article VII, Paragraph 3 in case of material breach of any terms of this DPA.

3. Priority of Agreements. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and individual acceptable use and privacy terms, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence, except that acceptable use terms shall prevail with regard to LEA's use of results of Services.

4. Notice. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein. Both parties shall notify the other of changes in contact information.

Irvine Unified School District	CSU/UC Mathematics Diagnostic Testing Project
Attn: Michelle Bennett	University of California, San Diego

5050 Barranca Parkway Irvine, CA 92604 Email: MichelleBennett@iusd.org	9500 Gilman Dr., #0112 La Jolla, CA 92093 Email: mdtp@ucsd.edu, with CC to pparsi@ucsd.edu

5. **Application of Agreement to Other Agencies.** Provider may agree by signing General Offer of Privacy Terms to be bound by the terms of this DPA for the services described therein for any Subscribing LEA who signs the General Offer of Privacy Terms at Exhibit E.

6. Entire Agreement. This DPA constitutes 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.

7. 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.

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

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

IRVINE UNIFIED SCHOOL DISTRICT

By: _____ Date: March 17, 2021

Printed Name: John Fogarty Title/Position: Asst Supt Business Services

IUSD Board Approved 3/16/2021

UNIVERSITY CALIFORNIA, SAN DIEGO

By: Jeff Warner Date: 2.23.2021

Printed Name: Jeff Warner Title/Position: Director, Ancillary Research Agreements

EXHIBIT "A"

DESCRIPTION OF SERVICES

The CSU/UC Mathematics Diagnostic Testing Project (MDTP) was jointly formed and supported by California State University (CSU) and University of California (UC) in 1977. The purpose of MDTP is to promote and support student readiness and success in college mathematics courses. MDTP achieves its purpose by developing diagnostic readiness tests aligned to the Common Core State Standards (CCSS) and supplying these diagnostic tools to secondary schools in California free of charge.

MDTP offers these free services through our online testing platforms or paper testing and scoring. Individual diagnostic reports are provided for students, and detailed item analyses and summary reports are provided for teachers. The student reports indicate areas in which students did well and those areas in which the test results suggest a need for further study in order to be prepared for future coursework. The summary reports have been used by teachers to help identify areas of the curriculum that seem to be working well and other areas or topics where changes may be needed.

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: MDTP	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred 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	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/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)	
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:	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	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	

EXHIBIT "C"
DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII")from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 177, SOPIPA, the term "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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of this DPA, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Student Data, metadata, and user or Pupil Generated Content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of this DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Pupil Records. Within the DPA the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 177, SOPIPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

School Official: For the purposes of this DPA and pursuant to 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 education records; and (3) Is subject to CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and Federal 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.

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

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Pupil Records. However, for the purpose of this Agreement, the term "Third Party" when used to indicator the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

ADDITIONAL DATA SECURITY REQUIREMENTS

Not applicable

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Irvine Unified School District and which is dated May 9, 2021 to any other LEA ("Subscribing LEA") who accepts this 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 other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CITE in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

UNIVERSITY CALIFORNIA, SAN DIEGO

By: Jeff Warner Date: 2.23.2021

Printed Name: Jeff Warner Title/Position: Director, Ancillary Research Agreements

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 Term. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW:

Name: _____

Title/Position: _____

Email Address: _____