

AN OVERVIEW OF THE CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Introduction: Since the passage of AB 1584, (now found at California Education Code section 49073.1), school districts have struggled to incorporate its required provisions in their contracts with digital providers. Two reasons account for a large portion of these difficulties. First, school districts often do not have the legal resources to negotiate with legally compliant privacy provisions, especially when they are negotiating with digital providers who may be resistant to change contract provisions the providers have crafted for their own purposes often at considerable expense. Second, other school districts are often reluctant to adopt the products for their school district, especially if they do not know whether these other agreements have been legally reviewed, and by persons who are comfortable in the new law of data privacy.

The California Student Data Privacy Agreement (referred to here as the "DPA") attempts to tackle these two challenges head on. First, it has been reviewed by several sets of legal and subject matter experts ranging from the Federal government, private attorneys, and educators working in the data privacy field both within the State of California and beyond. Users of this document can know, with a high degree of confidence, that it meets both the requirements of Federal and California State law.

School districts using this DPA for their digital contracts can, by uploading the executed DPA into the California Student Privacy Alliance ("CSPA") website, make the DPA available for use by other school districts. This includes school districts both within California and outside of California, since California is now a member of a nationwide data contract exchange maintained by the Student Data Privacy Consortium ("SDPC").

Practical Document: Legal compliance was not the only objective of the drafters of this DPA. They also sought to make this a practical and useful document; therefore this document contains provisions that will be of assistance to those persons, at the District and the Vendors who will administer the digital program established by the underlying agreement. We will briefly note some of the more important provisions of the DPA:

(a) *Nature of Digital Services:* Paragraph 2 of Article I of the DPA describes the service to be provided by the digital vendor. Such a description is often missing in many digital contracts. Having a short and workable summary of the services will also provide a description of the benefits of such a service to members of the educational community, a vital component in the acceptance and dissemination of educational digital products.

(b) *Types of Data to be Transferred:* Paragraph 3 of Article I, provides an opportunity for the Vendor and the District to list the types of student data that the providers will need in order to perform its services. This listing can be accomplished either by listing the types of data to be transferred in the text of the DPA or by checking the data "boxes" in Exhibit B, the Schedule of Data, attached to the DPA.

On Cover Page:

Locate fillable field **Insert Name Of School District or Local Education Agency** and insert the name of your LEA.

Locate fillable field **Insert Name of Provider** and insert the name of the Provider.

Locate fillable field **Date of Service Agreement** and insert the actual date of the agreement.

On Page 1:

Locate fillable field **Insert Name Of School District or Local Education Agency** and insert the name of your LEA.

Locate fillable field **Insert Name of Provider** and insert the name of the Provider.

Locate fillable field **Insert Date** and insert the date of the agreement.

Locate second fillable field **Insert Date** and insert the date of the agreement.

On Page 2:

Locate fillable field **Insert Brief Description of Services** and insert See Exhibit A or mark Not Applicable.

On Page 3:

Locate fillable field **Insert Categories of Student Data to be provided to the Provider** and insert See Exhibit B or mark Not Applicable.

On Page 8:

Locate fillable field **Insert County** and insert the name of the jurisdictional county.

On Page 9:

Locate fillable field **Insert Name of School District or LEA** and insert the name of the LEA.

Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the CDSPA.

Locate fillable field **Date of Service Agreement** and insert the date signed by the LEA.

Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the LEA.

Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the LEA.

Locate second fillable field **Insert Name of Provider** and insert the name of the Provider.

Locate second fillable field **Signature No Electronic Signatures Allowed** and manually sign the CDSPA.

Locate second fillable field **Date of Service Agreement** and insert the date signed by the Provider.

Locate second fillable field **Printed Name** and insert the name of the individual signing on behalf of the Provider.

Locate second fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Provider.

On Page 10:

Locate fillable field **Insert Detailed Description of Services Here** found as Exhibit A and insert Description of Services or mark Not Applicable.

On Pages 11-12:

Locate fillable fields **Check If Use By Your System** and check appropriate data element boxes.

On Page 16:

Locate fillable field **Insert Additional Data Security Requirements Here** found as Exhibit D and insert Data Security Requirements or mark Not Applicable.

For Providers who wish to sign the General Offer of Terms:

On Page 17 #1 Offer of Terms:

Locate fillable field **Insert Name of Initiating LEA** and insert the name of the initiating LEA.

Locate fillable field **Insert Date** and insert the date of the original initiating DPA.

Locate fillable field **Insert Provider Name** and insert the name of the Provider.

Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the General Offer of Terms.

Locate fillable field **Date** and insert the date signed by the Provider.

Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the Provider.

Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Provider.

For Subscribing LEAs who wish to accept the General Offer of Terms signed by a given Provider:

On Page 17 #2 Subscribing LEA (without making any changes to #1)

Locate fillable field **Insert Subscribing LEA Name** and insert the name of the LEA.

Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the General Offer of Terms.

Locate fillable field **Date** and insert the date the Subscribing LEA accepts the General Offer of Terms.

Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the Subscribing LEA.

Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Subscribing LEA.

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Dry Creek Joint Elementary School (hereinafter referred to as "LEA") and The Cooper Institute (hereinafter referred to as "Provider") on 5/22/19. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated 5/22/19 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy 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 Service Agreement conforms 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", agrees 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 pursuant to the Service Agreement, 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, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. 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:

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA.** LEA shall provide data for the purposes of the Service Agreement 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.
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
4. **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.

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 FERPA, COPPA, PPRA, AB 1584, and SOPIPA.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement 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 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.

obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices 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 pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
 - d. **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.
 - e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement
 - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.
2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process:
- a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "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 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.

destroy all of LEA's data pursuant to Article V, section 1(b).

4. **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 the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile 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.
6. **Application of Agreement to Other Agencies.** Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.
7. **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.
8. **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.
9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA,

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

The Cooper Institute

[Handwritten Signature]

Date: 5/22/19

Printed Name: ONYENA MACHEGE

Title/Position: CID

LEA: Dry Creek Joint Elementary School District

[Handwritten Signature]

Date: 9/4/17

Printed Name: James Ferguson

Title/Position: Asst. Supt. Admin Services

Note: Electronic signature not permitted.

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.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify: <i>fitness assessment data, activity assessment data</i>	<input checked="" type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications that are captured (emails, blog entries)	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input checked="" type="checkbox"/>
	Language information (native, preferred or primary language spoken by student)	<input checked="" type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input checked="" type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input checked="" type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
Other enrollment information-Please specify:	<input type="checkbox"/>	
Parent/Guardian Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	<input checked="" type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
Other indicator information-Please specify:	<input type="checkbox"/>	
Student Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Vendor/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>
Student work	Student generated content, writing, pictures etc.	<input type="checkbox"/>

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 1177, 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 the Service Agreement, 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

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 indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [redacted] and which is dated [redacted] to any other LEA ("Subscribing LEA") to anyone 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 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 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. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

[redacted] The Cooper Institute

[redacted] *Dyrelah*

Date: [redacted] 5/22/19

Printed Name: [redacted] DAMEKA NCHEGE

Title/Position: [redacted] CIO

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.

[redacted]

[redacted]

Date: [redacted]

Printed Name: [redacted]

Title/Position: [redacted]