

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Butte County Office of Education

and

Curriculum Associates, LLC

01/08/2018

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Butte County Office of Education (hereinafter referred to as "LEA") and Curriculum Associates, LLC (hereinafter referred to as "Provider") on 01/08/2018. 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 Exhibit A, Price Quote 120547.2; 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.

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.

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule 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 term used in the Service Agreement.

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 pursuant to the Service Agreement 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 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 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.** 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 Student generated content to a separate student account.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party 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 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.
5. **Ownership.** For the avoidance of doubt, LEA acknowledges and agrees that Provider's proprietary i-Ready® software solution and all intellectual property rights therein is owned solely and exclusively by Provider and, except for the licenses granted explicitly herein, nothing in this Agreement shall grant the LEA any right, title, and interest in or to the i-Ready® software solution.
6. **Limitations of Use.** The LEA shall not, nor permit any of its authorized users to: (a) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or algorithms underlying the Product; (b) modify, copy, translate, or create derivative works based on the Product or any of the content contained therein; (c) rent, lease, distribute, sell, resell, assign, or otherwise transfer rights to the Product; (d) use the Product for timesharing or services bureau purposes or otherwise for the benefit of a third party other than students or staff within the LEA's organization; or (e) remove any proprietary notices from the Product.

The LEA may not reproduce, upload, post, transmit, download or distribute any part of the

Product content or information, or information accessed at other sites through links made from the Product, other than printing out or downloading portions of the text and images for use in connection with the work of the LEA's organization. If the LEA's users leave the Product via a link to a third party site, Provider is in no way responsible for that third party site, and the LEA's use of that third party site will be governed by that site's terms of use, not this Agreement.

The LEA must use the Product in compliance with all applicable laws, rules and regulations, including, without limitation, laws and regulations that govern the export of technical data outside of the United States.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRRA, 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.
4. **No Disclosure.** Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.
5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement after written request and when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition, with the exception of backups that provider may maintain and destroy in accordance with its data handling policies in Exhibit D. 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. Provider shall provide written notification to LEA when the Data has been disposed. 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. Nothing in the Service Agreement authorizes Provider to maintain personally

identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider 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. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement after written request from LEA and when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree, except for backups which Provider may maintain and destroy in accordance with its data handling policies in Exhibit D. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition, except as otherwise expressed in this Service Agreement.
 - 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.
 - 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 District, Provider shall reimburse District for reasonable expenses associated with notifying 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**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider 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 so long as the Service Agreement has lapsed or has been terminated.

Effect of Termination Survival. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

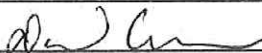
3. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license 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.
4. **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.
5. **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.

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and amends 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 Butte COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE 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.

Curriculum Associates, LLC

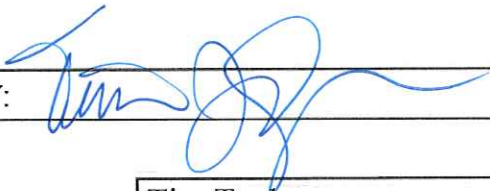
By: 

Date: 01/08/2018

Printed Name: David Caron

Title/Position: Chief Financial Officer

Butte County Office of Education

BY: 

3/22/18

Tim Taylor

Superintendent

Note: Electronic signature not permitted.

Curriculum Associates[®] LLC

Placing an Order

Please attach quote to all signed purchase orders.

- 1) **Email:** orders@cainc.com
- 2) **Fax:** 1-800-366-1158
- 3) **Mail:**
ATTN: CUSTOMER SERVICE DEPT.
Curriculum Associates, LLC
P.O. Box 2001
North Billerica, MA 01862-0901

Please visit www.curriculumassociates.com for more information about placing orders or contact CA's Customer Service department (1-800-225-0248) and reference quote number for questions.

Shipping Policy

Unless otherwise noted, shipping costs are calculated as follows.

Order amount	Percentage of Order
\$999.99 and less	12% with \$12.99 minimum freight charge
\$1,000 to \$4,999.99	10%
\$5,000 to \$99,999.99	8%
\$100,000 and more	6%

Please contact local CA Sales Representative, customer service (1-800-225-0248), or <http://www.curriculumassociates.com/> for expedited shipping rates.

Unless otherwise expressly indicated, the shipping terms for all deliveries is FOB CA's Shipping Point (whether to a CA or third party facility). Risk of loss and title is passed to purchaser upon transfer of the goods to carrier, standard shipping charges (listed above) are added to the invoice or included in the unit price unless otherwise specified.

Payment Terms

Payment terms are as follows.

- With credit approval: Net 30 days
- Without credit approval: Payment in full at time of order
- Accounts must be current before subsequent shipments are made

i-Ready[®]

Customer's use of i-Ready[®] shall be subject to the i-Ready Terms and Conditions of Use, which can be found at <http://www.i-ready.com/support/>.

Return Policy

Except for materials sold on a non-refundable basis, purchaser may return, at purchaser risk and expense, purchased materials with pre-approval from CA's Customer Service. Please examine your order upon receipt. Before returning material, call CA's Customer Service department (1-800-225-0248) for return authorization. When returning material, please include your return authorization number and the return form found on the back of your packing slip. i-Ready[®] and BRIGANCE[®] Online Management Systems may be returned for a pro-rated refund for the remaining time left on the contract. We do not accept returns on unused i-Ready licenses[®], individually sold Teacher Toolbox access packs, materials that have been used and/or are not in "saleable condition," and individual components of kits or sets including but not limited to Ready[®] Student Sets, Ready[®] Teacher Sets, and BRIGANCE[®] Kits.

For more information about the return policy, please visit <http://www.curriculumassociates.com/help/default.aspx?topic=188>.

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:	<input 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 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 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 type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input 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 type="checkbox"/>

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input checked="" type="checkbox"/>
	Low income status	<input checked="" 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 type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Vendor/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input 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 checked="" 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 type="checkbox"/>
Student work	Student generated content; writing, pictures etc.	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data -Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data - Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored or collected by your application	<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

Information in the Student's Email

Provider: For purposes of the Service Agreement, 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 Service Agreement 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 1177, 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.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement 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, or anonymous usage data regarding a student's use of Provider's services.

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

Exhibit D:

Data Handling and Privacy Statement

Purpose. Curriculum Associates takes the protection of our customers' data and information, particularly student data, very seriously. The purpose of this Data Handling and Privacy Statement is to inform Curriculum Associates' customers about its current data security policies and practices, which are intended to safeguard this sensitive information. Curriculum Associates handles customer data in a manner consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), the California Student Online Personal Information Protection Act (SOPIPA), and other state student data privacy protection laws.

Scope. This policy covers the collection, use, and storage of data that is obtained through the use of Curriculum Associates' proprietary i-Ready® online diagnostic and instructional platform and related services provided by Curriculum Associates.

Student Data Obtained and Collected. Curriculum Associates receives certain information from its school district customers to enable students to use i-Ready. The following information is generally provided to Curriculum Associates for each student user of i-Ready: student first and last name, date of birth, gender, ethnicity or race, student school enrollment, student grade level, teacher name, English language learner status, and eligibility for free- or reduced-price lunch. When students use i-Ready, certain assessment results and usage metrics are also created. These results and usage metrics are used by Curriculum Associates as described below. While teachers and school administrators are able to access student information and related i-Ready usage data, this information is not made available to other students or the public. Note that Curriculum Associates does not solicit personally identifiable information directly from students—all student information is provided by school district customers or created through the use of the i-Ready platform.

Use of Student Data. Curriculum Associates only uses student data for education-related purposes. Curriculum Associates only uses student-identifiable data provided by schools and/or school districts to make i-Ready available to that particular student, and to provide related reports and services to that student's school and school district and its teachers and administrators. Curriculum Associates uses student data collected from the use of i-Ready for the purpose of making i-Ready available to its customers and improving its content and effectiveness. Curriculum Associates collects and uses aggregated, de-identified student data for core product functionality to make i-Ready a more effective, adaptive product. "De-identified student data" refers to data generated from usage of i-Ready from which all personally identifiable information has been removed or obscured so that it does not identify individual students and there is no reasonable basis to believe that the information can be used to identify individual students. Curriculum Associates also uses de-identified student data for research and development purposes, including analyzing the efficacy of i-Ready. While some of this work is done internally, Curriculum Associates does share de-identified data with trusted third-party research partners as part of these research initiatives. Curriculum Associates does not attempt to re-identify de-identified student data and takes reasonable measures to protect against the re-identification of its

de-identified student data. It also prohibits its research partners from attempting to re-identify de-identified student data. Curriculum Associates does not sell student data or otherwise share student identifiable data with third parties. Curriculum Associates does not include advertisements within i-Ready nor does it use student data for targeted advertising in any manner.

Student Privacy Pledge. To further demonstrate its commitment to protecting the privacy of student information, Curriculum Associates has taken the Student Privacy Pledge <https://studentprivacypledge.org/>. This means that, among other things, Curriculum Associates has pledged not to sell student information, not to engage in behaviorally targeted advertising, and to use collected data for authorized purposes only. Curriculum Associates only uses collected student data for the purposes described in the previous paragraph.

Network-Level Security Measures. Curriculum Associates' i-Ready systems and servers are hosted in a cloud environment. Our hosting provider implements network-level security measures in accordance with industry standards. In addition, Curriculum Associates manages its own controls of the network environment.

Server-Level Security Measures. Access to production servers is limited to a small, identified group of operations engineers that are trained specifically for those responsibilities. The servers are configured to conduct daily updates for any security patches that are released and applicable. The servers have anti-virus, intrusion detection, configuration control, monitoring/alerting, and automated backups. In addition, Curriculum Associates conducts regular vulnerability testing.

Computer/Laptop/Device Security Measures. Curriculum Associates employs a full IT staff that manages and secures its corporate and employee IT systems. Laptops are encrypted and centrally managed with respect to configuration updates and anti-virus. Access to all Curriculum Associates computers and laptops is password-controlled. Curriculum Associates sets up teacher and administrator accounts for i-Ready so that they are also password-controlled.

Encryption. i-Ready is only accessible via https and all public network traffic is encrypted with the latest encryption standards. Encryption of data at rest is implemented for all data stored in the i-Ready system.

Employee and Contractor Policies and Procedures. Curriculum Associates limits access to student-identifiable data and customer data to those employees who need to have such access in order to allow Curriculum Associates to provide quality products and services to its customers. Curriculum Associates requires all employees who have access to Curriculum Associates servers and systems to sign non-disclosure agreements. Curriculum Associates requires its employees and contractors who have access to student data to participate in annual training sessions on IT security policies and best practices. Any employee who ceases working with Curriculum Associates is reminded of his or her non-disclosure obligations at the time of departure, and network access is terminated at that time.

Third-Party Audits and Monitoring. In addition to internal monitoring and vulnerability assessments, Curriculum Associates contracts with a third party to conduct annual security audits, which includes penetration testing of the i-Ready application. Curriculum Associates reviews the third-party audit findings and will implement recommended security program changes and enhancements where practical and appropriate.

Data Retention and Destruction. Student and teacher personal data is used only in the production systems and only for the explicitly identified functions of the i-Ready application. Student and teacher personal data is de-identified before any testing or research activities may be conducted. Upon the written request of a customer, Curriculum Associates will remove all personally identifiable student and teacher data from its production systems at the end of a contract. In addition, Curriculum Associates reserves the right, in its sole discretion, to remove a particular customer's student data from its production servers a reasonable period of time after its relationship with the customer has ended, as demonstrated by the end of contract term or a significant period of inactivity in all customer accounts. Student data is removed from backups in accordance with Curriculum Associates' data retention practices. If Curriculum Associates is required to restore any materials from its backups, it will purge all student-identifiable data not currently in use in the production systems from the restored backups.

Correction and Removal of Student Data. Parents of students who use i-Ready may request correction or removal of their child's personally identifiable data from i-Ready by contacting their students' teacher or school administrator. The teacher or school administrator can then verify the identity of the requesting party and notify Curriculum Associates of the request. Curriculum Associates will promptly comply with valid requests for correction or removal of student data; however, removal of student personally identifiable data will limit that student's ability to use i-Ready.

Breach Notification. Curriculum Associates follows documented "Security Incident Management Procedures" when investigating any potential security incident. In the event of a data security breach, Curriculum Associates will notify impacted customers as promptly as possible that a breach has occurred, and will inform them (to the extent known) what data has been compromised. Curriculum Associates expects customers to notify individual teachers and parents of any such breach to the extent required, but will provide customers reasonably requested assistance with such notifications and will also reimburse customers for the reasonable costs associated with legally required breach notices.

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Butte County Office of Education and which is dated 01/08/2018 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.

Curriculum Associates, LLC



Date: 01/08/2018

Printed Name: David Caron

Title/Position: Chief Financial Officer

2. Subscribing LEA

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

Butte County Office of Education



Date: 3/22/18

Printed Name: Tim Taylor

Title/Position: Superintendent