CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

SANTEE SCHOOL DISTRICT

and

Learning A-Z

Name of Service Provider

May 4, 2018

Date of Service Agreement

This California Student Data Privacy Agreement ("DPA") is entered into by and between the **SANTEE SCHOOL DISTRICT** (hereinafter referred to as "LEA") and Learning A-Z (hereinafter referred to as "Provider") on May 4, 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 a contract dated May 4, 2018 ("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 Federal Educational and Privacy rights Act ("FERPA") at 12 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 177 (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:

Online Curriculum resources

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 create a 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 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. **Sub-Processors**. Provider shall enter into written agreements with all Sub-Processors performing functions pursuant to the Service Agreement, whereby the Sub-Processors agree to be bound by 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 but not limited to 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.

4. **No Disclosure**. LEA 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. De-identified 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 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 of the date of termination and 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. 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 (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 Client.

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 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. 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. **Sub-Processors Bound**. Provider shall enter into written agreements whereby Sub-Processors agree to be bound to the same requirements and duties as set forth in Article IV of the Service Agreement and shall periodically conduct or review compliance monitoring and assessments of Sub-Processors 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 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**. 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.

3. **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).

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 Form of General Application 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, 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 [Insert County] 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.

Learning A-Z

[*Vendor Name*]

Signed: _____ Date: 5-4-18

Printed Name Paul Littlewood

Title/Position Sr. Vice President

SANTEE SCHOOL DISTRICT

Signed: _____ Date: 5/31/18

Printed Name: BERNARD YEO

Title/Position: DIR TECHNOLOGY

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[*INSERT DETAILED DESCRIPTION OF SERVICES HERE*]

Online curriculum resources

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users. Use of cookies etc.	✓
	Other application technology meta data-Please specify	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	✓
	Other assessment data-Please specify	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications 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	
	Teacher names	
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	
	State ID number	
	Vendor App assigned student ID number	
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content, writing, pictures etc	✓
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if used by your system
	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 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 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.

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.

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

Sub-Processor: For the purposes of this Agreement, the term "Sub-Processor" (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. 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"

DATA SECURITY REQUIREMENTS

[*INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE*]

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offer the same privacy protections found in this DPA between it and **SANTEE SCHOOL DISTRICT** and which is dated May 4, 2018 to any other LEA ("Subscribing LEA") who accepts this General Offer though 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 provide 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 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 the California Student Data Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Learning A-Z

[*Vendor Name*]

Signed: _____ Date: May 4 ,2018

Printed Name: Paul Littlewood Title/Position: Sr VP of Sales

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.

SANTEE SCHOOL DISTRICT

Signed: _____ Date: 5/31/18

Printed Name: BERNARD YEO Title/Position: DIR. TECHNOLOGY

Learning A-Z

A Cambium Learning Company

Alignment with CA AB-1584 Regarding Pupil Records

(a) A local educational agency may, pursuant to a policy adopted by its governing board or, in the case of a charter school, its governing body, enter into a contract with a third party for either or both of the following purposes:

(1) To provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

(2) To provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records in accordance with the contractual provisions listed in subdivision (b).

Learning A-Z (contracted third party of local educational agency) provides web-based educational learning software. In doing so, we access certain pupil records, and we follow the provisions as identified in subdivision b (outlined below).

(b) A local educational agency that enters into a contract with a third party for purposes of subdivision (a) shall ensure the contract contains all of the following:

(1) A statement that pupil records continue to be the property of and under the control of the local educational agency.

The District shall at all times retain ownership of pupil records. Learning A-Z makes no claim of ownership over pupil records.

(2) Notwithstanding paragraph (1), a description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil-generated content to a personal account.

To obtain pupil records, the pupil must contact the licensee and request that the licensee contact Learning A-Z in order to receive their data.

(3) A prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract.

Our privacy policy (that is accepted by each licensee prior to use) states that student data entered on the site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. Learning A-Z will not ask licensee to enter, and licensee is instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

We will only disclose student data to authorized employees or representatives of the LEA and will not knowingly disclose the student data to any third person without express written authorization. When, at the request of the LEA, Learning A-Z acquires assessment or other information, including personally identifiable student data, from a third party source Learning A-Z treats that information with the same confidentiality and security safeguards as though it were provided directly by the LEA. Additional agreements may be required by the third party to authorize transmission of data to Learning A-Z.

(4) A description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information.

To obtain and review pupil records, the pupil must contact the licensee and request that the licensee contact Learning A-Z in order to receive their data.

(5) A description of the actions the third party will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records. Compliance with this requirement shall not, in itself, absolve the third party of liability in the event of an unauthorized disclosure of pupil records.

Learning A-Z's approach to ensure the provisions of (5) include the following:

- Learning A-Z designates key leadership roles for product management and operations. These leaders are responsible for ensuring the maintenance of privacy measures consistent with corporate technical guidance.
- All Learning A-Z employees are subject to corporate non-disclosure agreements, which include provisions to ensure that all employees (and contractors) agree that any confidential information (including reference information) shall remain private to Learning A-Z.
- Learning A-Z employees participate in regular ethics training that includes continued emphasis on adhering to our business code of conduct that reinforces the agreements that have been made in the employment and/or work contracts.

(6) A description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records.

Learning A-Z's practice, should a breach of privacy occur, would be to contact the LEA to inform it of the particular situation. Learning A-Z would then rely upon the LEA to inform eligible pupils, parents, or lega guardians in accordance with their LEA's policies.

(7) (A) A certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced.

(B) Learning A-Z will use Student data to provide the service to the licensee's LEA. Learning A-Z will not keep the student data after the contract termination

Learning A-Z will use student data to provide the services to the licensee's LEA. Learning A-Z will not keep the student data after contract termination. Licensee may not disclose or otherwise use the student data entered on this site for any unauthorized purposes. An LEA may from time to time request that Learning A-Z provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that Learning A-Z is providing that data as the LEA's agent and that once the data is received by the third party, Learning A-Z no longer has any control over the use or disposition of the data.

(8) A description of how the local educational agency and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g).

FERPA requires limitations on disclosure of records and implementation of appropriate security measures to protect those records. To help LEAs comply with FERPA, Learning A-Z has adopted certain practices and requires that educators using this site fulfill certain responsibilities to safeguard student data:

- Only a minimum amount of personally identifiable student data required for the setup of the system is requested. Learning A-Z requires student first name, student last name, and student identification number. Additional data, not specific to the student, is also required to complete system setup, including the teacher first and last name, class name, grade level, and school name. Student

demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data and is obtained only with written permission from the licensee's LEA.

- Data Quality: Licensee is responsible for keeping student data that he/she enters accurate, complete and up-to-date. If he/she recognizes that student data is inaccurate, incomplete, or out-of-date, he/she is responsible for correcting it. If he/she experiences problems making corrections to student data, he/she is requested to notify Learning A-Z, and Learning A-Z will assist with making corrections.
- Security Safeguards: We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from licensees. We will implement reasonable and appropriate safeguards when collecting student data from licensee and when storing that student data in our database, and licensee will observe our security safeguards and exercise reasonable caution when using Learning A-Z's site.

Other FERPA-compliant measures are identified in 1–7 above.

Additionally, Learning A-Z operates in compliance with the Children's Online Privacy Protection Act ("COPPA"). The LEA hereby grants verifiable parental consent for the collection of personal information as defined by COPPA.

(9) A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

In the event that Learning A-Z wishes to release aggregated data that identifies the licensee's school or LEA by name, Learning A-Z will enter into a separate agreement with the LEA or licensee to authorize release and publication. Learning A-Z may also use aggregated data in its research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personally identifiable student data to market any products or services.

(c) In addition to any other penalties, a contract that fails to comply with the requirements of this section shall be rendered void if, upon notice and a reasonable opportunity to cure, the noncompliant party fails to come into compliance and cure any defect. Written notice of noncompliance may be provided by any party to the contract. All parties subject to a contract voided under this subdivision shall return all pupil records in their possession to the local educational agency.

Learning A-Z acknowledges and accepts this statement.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Deidentified information" means information that cannot be used to identify an individual pupil.

(2) "Eligible pupil" means a pupil who has reached 18 years of age.

(3) "Local educational agency" includes school districts, county offices of education, and charter schools.

(4) "Pupil-generated content" means materials created by a pupil, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content. "Pupil-generated

content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

(5) (A) "Pupil records" means both of the following:
(i) Any information directly related to a pupil that is maintained by the local educational agency.
(ii) 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 agency employee.
(B) "Pupil records" does not mean any of the following:
(i) Deidentified information, including aggregated deidentified information, used by the third party to improve educational products for adaptive learning purposes and for customizing pupil learning
(ii) (ii) Deidentified information, including aggregated deidentified information, used to demonstrate the effectiveness of the operator's products in the marketing of those products.
(iii) Deidentified information, including aggregated deidentified information, used for the development and improvement of educational sites, services, or applications.

(6) "Third party" refers to a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Learning A-Z acknowledges and accepts these definitions.

(e) If the provisions of this section are in conflict with the terms of a contract in effect before January 1, 2015, the provisions of this section shall not apply to the local educational agency or the third party subject to that agreement until the expiration, amendment, or renewal of the agreement.

Learning A-Z acknowledges and accepts this statement.

(f) Nothing in this section shall be construed to impose liability on a third party for content provided by any other third party.

Learning A-Z acknowledges and accepts this statement.

Sr. Vice President of Sales
May 4, 2018