CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Vista Unified School District

and

Ellevation Inc.

06/21/2018

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Vista Unified School District (hereinafter referred to as "LEA") and Ellevation Inc. (hereinafter referred to as "Provider") on . 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 4/19/2018 ("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 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:

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":

See Attached Exhibit B and Exhibit B-1

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.

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.

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 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 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 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. **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 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 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,

WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN San Diego COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS 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.

Ellevation Inc.

Edward Rice

Date: 06/21/2018

Printed Name: Edward Rice

Title/Position: President

Vista Unified School District

Donna Caperton

Date: 06/21/2018

Printed Name: Donna Caperton

Title/Position: Assistant Superintendent, Business Svcs

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Ellevation is a mission-driven web-based software company focused exclusively on English Language Learners (ELLs) and the educators that serve them. Ellevation offers school districts in California two software solutions that can be purchased individually or together
Ellevation.
Ellevation for California, puts all information and data about ELLs in one place, helping educators enhance instruction, save time, and improve collaboration. Ellevation includes our industry-leading Monitoring Center, a variety of dashboards that make student data actionable, and over 50 pre-developed ELL-focused reports and letters, including letters to parents that can be generated in 35 different languages.
Ellevation Strategies offers a digital library of curated activities and strategies designed to help classroom teachers personalize instruction for ELLs across all grades and content areas.

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.	✔

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	
Transcript	Student course grades	✔
	Student course data	✔
	Student course grades/performance scores	✔
	Other transcript data -Please specify:	

Category of Data	Elements	Check if used by your system
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 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 SECURITY REQUIREMENTS

Securing our Partners' Personally Identifiable Information (PII) is Ellevation's highest priority. Ellevation's data security policy is comprised of several important components, each of which is include in Exhibit D-1. Ellevation maintains a formal internal WISP (Written Information Security Policy) as well as a formal Data Privacy Policy.

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Ellevation Inc. and which is dated [ ] to any other LEA ("Subscribing LEA") to anywho 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 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.

Ellevation Inc.

[signature]

Date: 6/21/2017

Printed Name: Edward Rice

Title/Position: President

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.

[ ]

[ ]

Date: [ ]

Printed Name: [ ]

Title/Position [ ]

ELLEVATION

Exhibit B-1

Ellevation Data Specifications and Policy Guidance

Overview

Ellevation supports the import of various types of data; reducing the need for manual data entry. This process comprises three main steps:

1. The district data specialist will prepare the data files and send them to Ellevation.
2. Ellevation will receive, analyze, and manually import these files into the district database.
3. Once these initial files have been imported, Ellevation staff will work with the school district to automate the data update process. This process ensures that updates made in district's Student Information Systems are automatically reflected in Ellevation.

Ellevation Data Types:

- Student Demographics
- Staff Roster
- Student Schedules
- Student ELP Scores

Resources:

- Best Practices

Frequently Asked Questions (FAQ)

⚠ How to do we upload Files to Ellevation?

For **one-time file imports**, districts can upload information to one of our secure file-sharing portals, our SFTP server or ShareFile. We will download the files and evaluate them to make sure that they are usable and that they meet our minimal file format requirements. Then, we will import the files into Ellevation.

Ellevation will provision credentials for districts to connect to our SFTP server, which supports both **one-time** and **automated imports**. District data specialists will use those credentials to connect to this server and transfer files they've prepared to Ellevation over an encrypted and secure connection. Then, Ellevation will download the files and evaluate them. We will assess those files to make sure that they are usable and meet our minimal formatting requirements. Last, we will manually import those files into the Ellevation database.

During **automation setup**, Ellevation will support districts in using a combination of FTP clients, scripts, and job schedulers in the process of exporting from Student Information Systems and transferring updated student information to the SFTP server on a daily basis (M-F). Once we are receiving files on an automated schedule, we will set up a corresponding automation on the Ellevation side to download, pre-process, and import those files. This way, districts' data can be continually updated to be as accurate as possible in Ellevation.

Note: *In order to maintain FERPA compliance,* ***please do not*** *send data files to Ellevation via the Help Desk, Mavenlink, or email.*

ELLEVATION

⚠ What is the Preferred File Format and Extension?

We've found partners have the greatest success when working with **tab-delimited** (TXT) files.
Comma-separated values (CSV) files where values are wrapped in double-quotation marks are also acceptable.
We strongly recommend sending a TXT or CSV file, however if an Excel (XLS or XLSX) file is required we will review on a case by case basis. Fixed width files are NOT supported with the exception of official test score files.

⚠ What is the preferred file naming convention?

Please include the export type in your file names. For example: "student-demographics.txt"

Student Demographics

The student demographics data file is used to initially add students to Ellevation and to continually update their records. The data set should include:

- **ELL Specific Students (Preferred):**
  1. Current ELL students
  2. Former ELL students that are being monitored
  3. Former ELL students that have completed the mandated years of monitoring
  4. Never identified students (Were initially tested but not deemed ELL)
- **OR All Students (Okay)**: If your Student Information System does not allow you to export a subset of students, please specify which data field(s) can be used to determine which students are ELL. *Note: Ellevation does not upload students that are English Only.*

Student Demographics Specifications:

The list below shows the typical student data fields Ellevation currently supports. You may decide how few or how many of these fields are to be uploaded, with the exception of required fields. Refer to the **Sample File** for examples of what the field values would commonly look like. Please note that:

- Each student record must be on a ***separate row***. A student should ***only appear once*** in each file.
- Many of these ***fields can be omitted if the data isn't needed or is unavailable*** in your SIS.
- Ellevation can also look at differences in the student demographics files between import jobs, and can ***deactivate any students who no longer appear in the file for a subsequent update***. This ensures that students who graduate/withdraw/drop out/etc no longer appear as Active in Ellevation.
- If there are ***additional data fields*** that you want to load, they may be able to be mapped to special custom fields in Ellevation. For example, Free Lunch Program Status is not on the list, but if you wanted to make it available to Ellevation users, it could be uploaded into the Ellevation database as a Custom Flag.

Field * *Indicates required field*	**Notes** ⚠ *Indicates must read notes*
Student Demographics	
First Name *	*Example:* Angel
Middle Name	*Example:* Luis
Last Name *	*Example:* Hernandez
Active Status*	*Example:* Yes **Available Values**: Any Binary (Yes/No, Y/N, 1/0, etc) ⚠ Only required if file includes active and inactive students. Active Status is used to determine whether or not a student is actively enrolled in the school district (not whether or not he/she is enrolled in ELL programming).
LEA School Code *	*Example:* 432

	⚠ Required unless School Name is provided
School Name *	*Example:* Davis Elementary ⚠ Required unless LEA School Code is provided
Alternate School	*Example:* Washington High School or 122
ESL Teacher ID	*Example:* 123456 ⚠ Provide Staff ID# and name in separate columns. To bring in additional staff or schedule data please see respective sections below
ESL Teacher Name	*Example: Jane Smith* ⚠ Provide Staff name and Staff ID in separate columns
District Local ID *	*Example:* 12345 ⚠ Required if Testing ID not present. Local ID must be unique to student
State Testing ID *	*Example:* 123456789 ⚠ Required if Local ID not present. Testing ID must be unique to student and often used as unique identifier when loading assessment data
Grade Level *	*Example:* 6 **Available Values**: Blank, Pre-K, K, 1-13, Graduated
Gender	*Example:* Male **Available Values**: Male, Female
Date of Birth	*Example:* 3/23/2001
Address Line 1	*Example:* 123 Rose Street
Address Line 2	*Example:* #5
City	*Example:* Wilson
State	*Example:* NC
Zip Code	*Example:* 12345
Home Phone Number	*Example:* 111-123-4567
Cell Phone Number	*Example:* 111-123-4567

City/Town of Birth	*Example:* Mexico City
Birth Country (Nationality) *	*Example:* Mexico ⚠ Often required for state reporting
Native Language *	*Example:* Spanish ⚠ Required unless Home Language is provided
Home Language *	*Example:* English ⚠ Required unless Native Language is provided
Ethnicity *	*Example:* Hispanic **Available Values:** Hispanic, Not Hispanic ⚠ Often required for state reporting
Race *	*Example:* Asian **Available Values:** American Indian, Asian, Black, White, Pacific ⚠ Often required for state reporting
Designation & Status ⚠ We require at least one of the following pairs of data fields	
Initial Date Entered LEP AND Date Exited LEP/Date Monitoring Started *	*Example:* 8/25/2014 ⚠ Two date columns are required for this method of importing student designations and status
LEP Status inclusive of monitoring year *	*Example:* Current ELL **Typical Values**: Current ELL, Monitored Yr.1, Monitored Yr. 2, Monitored Yr.3, Monitored Yr. 4, Fully Exited, Tested Did Not Qualify ⚠ This method must include specific monitored year, not just a generic monitored status
LEP Status AND Monitoring Status *OR* Date Exited LEP/Date Monitoring Started *	*LEP Status Example:* Current ELL **Typical Values**: Current ELL, Monitored, Fully Exited, Tested Did Not Qualify AND *Monitoring Status Example:* Monitored Year 2 **Typical Values**: Monitored Yr.1, Monitored Yr. 2, Monitored Yr.3, Monitored Yr. 4, Not Monitored

	OR *Date Exited LEP/Date Monitoring Started Example:* 8/25/2014 ⚠ Two columns are required for this method of importing student designations and status, one status field and one either monitoring status OR date field
Key Dates ⚠ We prefer that dates be in mm/dd/yyyy format, if possible	
Date Entered US *	*Example:* 5/1/2014 ⚠ Often required for state reporting
Date Enrolled in the US *	*Example:* 8/12/2014 ⚠ Often required for state reporting
Date Enrolled in the District *	*Example:* 8/12/2014 ⚠ Often required for state reporting
Home Language Survey	*Example:* 6/1/2014
Parent Granted Permission	*Example:* 8/15/2014
Parent Denied Permission	*Example:* 8/15/2014
Date Withdrawn	*Example:* 5/1/2014
Date Graduated	*Example:* 5/1/2014
Date Dropped Out	*Example:* 5/1/2014
Years in US Schools *	*Example:* 2 **Available Values**: Customizable for up to 9 labels ⚠ Often required for state reporting
Status Flags ⚠ All Status Flags allow only binary Yes/No values	
Homebound	*Example:* No
Migrant	*Example:* No
Immigrant	*Example:* No
NOM	*Example:* Yes

Refused ESL/ELD Services	*Example:* No ⚠ Can be determined using LEP status field
Dropped Out	*Example:* No
Graduated	*Example:* No
Withdrawn	*Example:* No
Deceased	*Example:* No
Homeless	*Example:* No
Gifted and Talented	*Example:* No
Bilingual	*Example:* Yes
Dual Language Program	*Example:* Yes
IEP *	*Example:* Yes
504	*Example:* No
SIFE	*Example:* Yes
Parent Info	
Father Name	*Example:* John Smith
Father Phone	*Example:* 555-123-4567
Father Email	*Example:* johns@email.com
Father Workplace	*Example:* Consolidated Industries
Father Needs Interpreting	*Example:* Yes
Mother Name	*Example:* Jane Smith
Mother Phone	*Example:* 555-345-6789
Mother Email	*Example:* Janes@email.com
Mother Workplace	*Example:* Consolidated Industries
Mother Needs Interpreting	*Example:* No
Emergency Contact Name	*Example:* Jane Smith
Emergency Contact Phone	*Example:* 555-345-6789

Emergency Contact Email	*Example:* Janes@email.com
Emergency Contact Needs Interpreting	*Example:* No
Guardian Name	*Example:* Sam Smith
Guardian Phone	*Example:* 555-345-6789
Guardian Email	*Example:* Sams@email.com
Guardian Needs Interpreting	*Example:* No
Other	
Special Education/EC Info	*Example:* Hearing impairment **Available Values:** Autism, Deafness, Deaf-blindness, Developmental delay, Emotional disturbance, Hearing impairment, Intellectual disabilities, Multiple disabilities, Orthopedic, impairment, Other health impairment, Qualified with disabilities under 504, Specific learning disability, Speech or language impairment, Traumatic brain injury, Visual impairment
Comment	*Example:* Student shows excellent progress ⚠ Freeform text field

Staff Roster

The staff roster data file is used to associate educators with their ELL students in Ellevation. The data set should include:

- **All Active Staff**: If desired, the data could be pre-filtered by the district to only include instructional staff and administrators.

Staff Roster Specifications:

The list below shows the typical staff data fields Ellevation currently supports. You may decide how few or how many of these fields are to be uploaded, with the exception of required fields. Refer to the Sample File for examples of what the field values would commonly look like. Please note that:

- This process ***does not create user accounts*** in Ellevation, but merely populates a full list of staff who *could* become users in Ellevation via invitation from an administrator or through self-registration.
- Ellevation can also look at differences in the staff file between import jobs, and can ***deactivate any users who no longer appear in the file for a subsequent update***. This ensures that employees who are no longer associated with the district will no longer have access to Ellevation if they had accounts provisioned for them in the past.

Field * *Indicates required field*	Notes ⚠ *Indicates an important note*
Staff ID *	*Example*: 123456 ⚠ Staff ID must be unique to each person and consistent with the Staff IDs found in the Student Schedules File
Staff Email Address *	*Example*: johndoe@summerville.k12.aa.us ⚠ Staff Email Address must be a valid, unique, district-associated email address.
First Name *	*Example*: John
Last Name *	*Example*: Doe
School LEA Code *	*Example*: 345 ⚠ Required unless School Name is provided ⚠ For teachers with multiple school assignments, list the staff member in multiple rows (same Staff ID) with one school assignment per row
School Name *	*Example*: Lincoln Elementary ⚠ Required unless LEA School Code is provided
Role	*Example*: Other Educator ⚠ **Available Values**: ELL Teacher, Classroom Teacher, Other Educator, Administrator, or Non-Teacher
Group	*Example*: Users ⚠ Groups are used to more efficiently and effectively assign platform users and to facilitate filtering within the platform

Student Schedules

The student schedules data file populates students' course schedules into Ellevation and is used to associate educators with their ELL students in many areas across the Ellevation platform. A specific student schedule should include one or more courses and teachers, each pair associated with a specific class or period. Current course schedules are prefered, but full year schedules are accepted as long as all course include a term indicator.

Student Schedules Specifications:

The list below shows the typical schedule data fields Ellevation currently supports. You may decide how few or how many of these fields are to be uploaded, with the exception of required fields. Refer to the **Sample File** for examples of what the field values would commonly look like. Please note that:

- Ellevation allows ***up to four custom schedule-related fields*** of information to be stored (e.g. Duration).
- The schedule data file will ***only load schedule data for students who are already in Ellevation***. If the file contains schedule information for students who are not in Ellevation, that data will be skipped during the upload process.
- All existing entries for a student are ***replaced*** by the entries in the most recent student schedule data load.
- Ellevation supports the filtering of semester and full year courses.

Field * *Indicates required field*	**Notes** ⚠ *Indicates an important note*
Local Student ID *	*Example*: 123456 ⚠ Required if Testing ID not present. Local ID must be unique to student and consistent with the Local IDs found in the Student Demographics File
State Testing ID *	*Example*: 123456789 ⚠ Required if Local ID not present. Testing ID must be unique to student and consistent with the Testing IDs found in the Student Demographics File
Staff ID *	*Example*: A9483 ⚠ Staff ID must be unique to person and consistent with the Staff IDs found in the Staff Roster File
Teacher Name	*Example*: John Doe
Course Name *	*Example*: Science
Course Period	*Example*: 2
Course Code	*Example*: A123
Term *	*Example: Term 1*

	⚠ Required if sending full year schedule. Ellevation will map district values to Term 1, Term 2, or Full Year

Student ELP Scores

The student ELP scores data file is used to import students' initial and summative ELP test scores into their records in Ellevation. We ask districts to send at least two years of historical ELP test scores in addition to the current year's score file(s). Districts can send ELP test scores for a number of assessments, including WIDA ACCESS for ELLs (2.0 and earlier) and W-APT, CELDT, CELLA, NYSESLAT, TELPAS, IPT, LAS Links, ELDA, and more. Ellevation can import students' ELP score files produced by:

- **Testing Agency (Preferred)**: Testing agencies typically offer data exports upon request. For example, MetriTech and the DRC have predefined formats for their WIDA test scores (WAPT and ACCESS). Contact your testing agency for more information about the availability of ELP test score exports in a ***standardized format***.
- **OR State Department of Education:** The central education office for some state governments distribute test scores back to districts in a ***standardized format***. For example, the Texas Education Agency has predefined formats for TELPAS.
- **OR District SIS**

Student ELP Score Specifications:

Each assessment type has differences in terms of the scores captured for ELLs. However, the fields below reflect the typical ELP test data fields Ellevation currently supports. You may decide how few or how many of these fields are to be uploaded, with the exception of required fields. Refer to the **Sample File** for examples of what the field values would commonly look like. Please note that:

- ***Each row contains the score results from a single assessment date for an individual student.*** Multiple scores for a single assessment date cannot be on multiple rows.
- As each type of ELP assessment has different business rules and scores captured, a ***separate data file should be provided for each type of ELP assessment*** (ie: screener in one file, annual ELP assessment in another) ***and each year of scores***.
- ELP score data will ***only be loaded for students who are already in Ellevation***. If the file contains information for students who are not in Ellevation, that data will be skipped during the upload process.

Field * *Indicates required field*	**Notes** ⚠ *Indicates an important note*
District Local ID *	*Example:* 34567 ⚠ Required if Testing ID not present. Local ID must be unique to student and consistent with the Local IDs found in the Student Demographics File
State Testing ID *	*Example:* 123456789 ⚠ Required if Local ID not present. Testing ID must be unique to student and consistent with the Testing IDs found in the Student Demographics File
Date Given *	*Example:* 03/06/2014

Grade Level *	*Example:* 3 ⚠ Grade level must reference the student's grade when the test was administered to the student.
Test Administrator	*Example:* John Smith
Test Purpose	*Example:* Initial **Available Values**: Initial, Screener, Annual
Domain Raw Score	*Example:* Listening Raw Score of 100
Domain Scale Score	*Example:* Reading Scale Score of 90
Domain Proficiency Level	*Example:* Composite Proficiency Level of 4

Best Practices

In order to facilitate the import of district data files into Ellevation, we have a few best practices for districts to follow. These guidelines, when followed, can reduce back-and-forth between our teams and expedite the import process.

Practice	Details
Headers	If possible, please include the *header row* in all files transferred to Ellevation. Alternatively, please provide a list of all column headers in the order they appear in your files.
LEP Information	If sending multiple columns that include LEP-related information in the Student Demographics file, *please specify which column(s) should be used* for determining ELP Designation, LEP Status, Monitoring Status, LEP Dates and Receiving Services. Often, some of these fields are consistently maintained in the SIS and others are not. If there is any contradictory LEP-related information in the files, we will need to know which columns are accurate and which should be ignored.
Which students to send	If possible, please send information on *only your district's LEP student population*, in the Student Demographics file. Alternatively, you may send records for all students, but please specify which column(s) are used to determine which students are to be included in Ellevation (LEP, monitored, and exited students).
Dates	If possible, please send all dates in *mm/dd/yyyy format*.
Merging Files	If possible, please *merge all files of the same type that use the same headers into one file.* For example, as opposed to sending one Schedule file per school, please send one file that includes all students' schedules from all schools in the district.
Whitespace	Please *avoid including any leading or trailing whitespace* in both column headers and values.
Concatenate Guardian Names	If possible, in the Student Demographics file, for Mother Name, Father Name, Guardian Name, and Emergency Contact fields, please *send first and last names concatenated together* into one column. *For example:* Mother_Name = Jane Smith *As opposed to:* Mother_First_Name = Jane Mother_Last_Name = Smith

Separate Mailing Address	If possible, in the Student Demographics file, please *separate mailing address information into multiple columns*: Street Address Line 1, Street Address Line 2, City, State, Zip Code
Pivot Data (ELP Test Scores)	To allow for import into Ellevation, there can only be one student per row. That row should contain all domain, proficiency level, and scale scores for a single test date in separate columns. If your ELP score file contains multiple rows per student with each score for the same test in a separate row, please try to *pivot the file from multi-row to multi-column* (or long to wide) before sending.
Unique Records Only	Students and staff who are duplicated in files will be skipped during the import process. Please *drop duplicates to retain unique records* before sending.
Remove Metadata	Often, during the export from an SIS, metadata may be appended to the header or the footer of a file. The is typically a single, identifiable row at the beginning or end. If possible, please *remove this metadata* before sending the files.
Replace NULL Values	If possible, please *replace NULL values with empty strings* before sending files.
Binary Values	For binary fields, Ellevation accepts Yes/No, Y/N, 1/0, etc

ELLEVATION
Indispensable Tools for Today's ELL Professionals

Exhibit D-1

Securing our Partners' Personally Identifiable Information (PII) is Ellevation's highest priority. Ellevation's data security policy is comprised of several important components, each of which is summarized below. Ellevation maintains a formal internal WISP (Written Information Security Policy) as well as a formal Data Privacy Policy.

Corporate Security Policy

Ellevation has a set of company policies that enforce best practices for employees and subcontractors when accessing, communicating or handling potentially sensitive customer data in either electronic or paper format.

Application & Data Security

Ellevation uses a single-tenant policy for its customer data. Each district has its own dedicated database for its student, teacher, school, and test score data. End user-specific login IDs and password credentials ensure that users can only access their school's data (and, if desired, only certain sets based on permissions/role).

Ellevation products use a permissions-based security model that enables fine-grained access control at the user, school, role or district level. For example, district administrators can manage additional user accounts and generate reports for separate sets of students across the district, while classroom teachers may have "read-only" permission on the students on their course schedule. Specialists may have read-write access to certain portions of student records associated with one or more schools.

Application access requires use of the HTTPS or SFTP protocol, ensuring that data sent between the end user and the Ellevation platform is secure in transit and can only be decrypted by Ellevation. SSL security verifies that Ellevation is the only authorized recipient of said data. All SSL certificates use a minimum bit length of 2048 and SHA-2 hashing. Ellevation will provide a "whitelist" of all required domains in order to support any partner firewall requirements.

Operational Security

Ellevation maintains a persistent history of record-level access to records which user(s) may have accessed the data for a particular student in the Ellevation platform. Sensitive data at rest is encrypted using a minimum 256-bit key which is only accessible by authorized Ellevation employees. Ellevation employees who do have access to student data undergo security background checks and are required to use two-factor authentication.

Physical and Environmental Security

Per Ellevation's corporate security policy, access to the company's office is strictly managed and all employees are required to adhere to FERPA and related guidelines describing the use of student data. Operational access to production servers hosted at the Rackspace data centers (see http://www.rackspace.com/security/) or Amazon EC2 (see http://aws.amazon.com/security/) is restricted to authorized employees and support staff only. As part of their company's standard security policies, Amazon and Rackspace employees are not authorized to have file- or data-level access to Ellevation servers.

Regulatory Compliance

Given the sensitive nature of student data, including (but not limited to) accommodations, test scores, demographic and other educational information, access to student data in the Ellevation application is tightly controlled. Ellevation operates under the "school official" provision of FERPA and follows related industry best practices for handling PII and other sensitive student data. In accordance with the policies and regulations defined in FERPA, Ellevation requires expressed, written consent from an authorized school or district representative before we accept or release any type of student data. Ellevation also engages an independent third-party security firm to perform application and network security and penetration testing on an annual basis.