

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 2.0 (September 26, 2018)

School District/Local Education Agency:

Oak Grove School District

AND

Provider:

Ellevation Inc

Date:

08/01/2019

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the **Oak Grove School District** (hereinafter referred to as “LEA”) and **Ellevation Inc** (hereinafter referred to as “Provider”) on **08/01/2019**. 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 **08/01/2019** (“Service Agreement”); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (“SOPIPA”) found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; 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” (Exhibit “E”), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:

Ellevation software and professional development

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided 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 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 Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data 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 Student Data in 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 timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data 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 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.** If pupil generated content is stored or maintained by the Provider as part of the Services, described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
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.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.
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. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.
5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the

Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student 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. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

- a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.
 - b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.
6. **Advertising Prohibition.** Provider is prohibited from using or selling 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; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, 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 Exhibit "F" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in 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. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

- b. **Destruction of Data.** Provider shall destroy or delete all Student 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 the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards 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 digital 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, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
 - f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, 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.
 - h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
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, and not exceeding forty-eight (48) hours. 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. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said

written incident response plan.

- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, 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. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

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 in 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.
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. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
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), and Article II, section 3, above.
4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the 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, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:
 - a. **Designated Representatives**
The designated representative for the LEA for this Agreement is:
Name: Najeeb Qasimi
Title: The Director of IT
Contact Information:

6578 Santa Teresa Blvd
San Jose, CA 95119
(408) 227-8300

The designated representative for the Provider for this Agreement is:

Name: **Ellevation Inc**
Title: **President and Co-Founder**
Contact Information:
38 Chauncy Street, Fl 9
Boston
6173075755

- b. **Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: **Edward Rice**
Title: **President and Co-Founder**
Contact Information:
38 Chauncy Street, Fl 9
Boston, MA 02111
6173075755

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND


CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[Signature Page Follows]

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

Provider: Ellevation Inc

BY: 

Date: 06/25/2019

Printed Name: Ellevation Inc, Edward Rice

Title/Position: President and Co-Founder

Local Education Agency:

BY: 

Date: 06/25/19

Printed Name: Najeed Qasimi

Title/Position: Director

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Ellevation data management platform for educators working with ELLs. Ellevation strategy and collaborate and instructional tool for classroom teachers

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 program	✓
	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	✓
Schedule	Student scheduled courses	✓
	Teacher names	✓
Special Indicator	English language learner information	✓
	Low income status	✓
	Medical alerts/health data	

	Student disability information	✓
	Specialized education services (IEP or 504)	✓
	Living situations (homeless/foster care)	✓
	Other indicator information-Please specify:	
Student Contact Information	Address	✓
	Email	✓
	Phone	✓
Student Identifiers	Local (School district) ID number	✓
	State ID number	✓
	Provider/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	✓
	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 on the next page each additional data element used, stored or collected by your application	

No Student Data Collected at this time ____.

* Provider shall immediately notify LEA if this designation is no longer applicable.

Other: Use this box, if more space is needed.

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 Provider 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.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: 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 applicable state statutes.

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 Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

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 DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

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 LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

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 34 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 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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

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.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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.

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" 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"

DIRECTIVE FOR DISPOSITION OF DATA

Oak Grove School District directs Ellevation Inc to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

<u>Extent of Disposition</u> Disposition shall be:	<input type="checkbox"/> Partial. The categories of data to be disposed of are as follows: <input checked="" type="checkbox"/> Complete. Disposition extends to all categories of data.
<u>Nature of Disposition</u> Disposition shall be by:	<input checked="" type="checkbox"/> Destruction or deletion of data. <input type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
<u>Timing of Disposition</u> Data shall be disposed of by the following date:	<input type="checkbox"/> As soon as commercially practicable <input checked="" type="checkbox"/> By (Insert Date) <u>08 /30 /2022</u>

Authorized Representative of LEA



Verification of Disposition of Data
by Authorized Representative of Provider

Date

6/25/19

Date

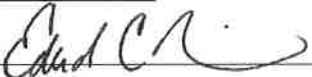
EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Oak Grove School District** and which is dated 08/01/2019 to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (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 CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: **Ellevation Inc**

BY: 

Date: **06/25/2019**

Printed Name: **Ellevation Inc**, Edward Rice

Title/Position: **President and Co-Founder**

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.

Subscribing LEA:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

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

Name: **Edward Rice**

Title: **President and Co-Founder**

Email Address: **sales@ellevationeducation.com**

EXHIBIT "F" DATA SECURITY REQUIREMENTS

see exhibit D-1

00618-00001/4274378.1



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.



△ 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: 8/26/2014

△ 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 *	<i>Example: 8/1/2014</i> △ Often required for state reporting
Date Enrolled in the US *	<i>Example: 8/12/2014</i> △ Often required for state reporting
Date Enrolled in the District *	<i>Example: 8/12/2014</i> △ Often required for state reporting
Home Language Survey	<i>Example: 8/1/2014</i>
Parent Granted Permission	<i>Example: 8/15/2014</i>
Parent Denied Permission	<i>Example: 8/15/2014</i>
Date Withdrawn	<i>Example: 8/1/2014</i>
Date Graduated	<i>Example: 8/1/2014</i>
Date Dropped Out	<i>Example: 8/1/2014</i>
Years in US Schools *	<i>Example: 2</i> 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	<i>Example: No</i>
Migrant	<i>Example: No</i>
Immigrant	<i>Example: No</i>
NOM	<i>Example: Yes</i>



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	<i>Example: Janes@email.com</i>
Emergency Contact Needs Interpreting	<i>Example: No</i>
Guardian Name	<i>Example: Sam Smith</i>
Guardian Phone	<i>Example: 555-345-6789</i>
Guardian Email	<i>Example: Sams@email.com</i>
Guardian Needs Interpreting	<i>Example: No</i>

Other

Special Education/EC Info	<i>Example: Hearing Impairment</i>
---------------------------	------------------------------------

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	<i>Example: Student shows excellent progress</i>
---------	--

 Freeform text field

Staff Roster

The staff roster data file is used to associate educators with their ELL students in Elevation. 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 Elevation 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 Elevation, but merely populates a full list of staff who **could** become users in Elevation via invitation from an administrator or through self-registration.
- Elevation 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 Elevation if they had accounts provisioned for them in the past.



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



Student Schedules

The student schedules data file populates students' course schedules into Elevation and is used to associate educators with their ELL students in many areas across the Elevation 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 preferred, 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 Elevation 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:

- Elevation 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 Elevation*. If the file contains schedule information for students who are not in Elevation, 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.
- Elevation supports the filtering of semester and full year courses.

Field	Notes
* Indicates required field	△ 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 Elevation. 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. Elevation 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 Elevation 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 Elevation.* If the file contains information for students who are not in Elevation, that data will be skipped during the upload process.

Field	Notes
* Indicates required field	⚠ 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: 03/09/2014



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 80

Domain Proficiency Level

Example: Composite Proficiency Level of 4



Best Practices

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



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 Elevation, 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. This 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, Elevation accepts Yes/No, Y/N, 1/0, etc



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.

