

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 2.0 (September 7, 2018)

School District/Local Education Agency:

Oak Grove School District

AND

Provider:

WestEd

Date:

02/27/2019

This California Student Data Privacy Agreement ("DPA") is entered into by and between the **Oak Grove School District** (hereinafter referred to as "LEA") and **WestEd** (hereinafter referred to as "Provider") on **02/27/2019**. 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 **02/27/2019** ("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:

See exhibit A

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 "E" 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: Mike Neuenfeldt

Title: Deputy CEO

Contact Information:

730 Harrison Street
San Francisco, CA 94107
4156153136

- 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: Mike Neuenfeldt

Title: Deputy CEO

Contact Information:

730 Harrison Street
San Francisco, CA 94107
4156153136

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: WestEd


BY:  _____

Date: 03/15/2019

Printed Name: Mike Neuenfeldt

Title/Position: Deputy CEO

Local Education Agency:

BY:  _____

Date: 4/2/19

Printed Name: Najeeb Qasimi

Title/Position: Director

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

See attached MOU



Memorandum of Understanding

Between

Oak Grove School District and WestEd

Social Skills Training Pilot Study (SST Pilot Study)

This Memorandum of Understanding (MOU) is made as of November __, 2018, by and between Oak Grove School District located in San Jose, CA, (District) and WestEd, a California joint powers agency with principal offices in San Francisco, California, regarding the study for the *Social Skills Study* ("SST Pilot Study" or "Study"). This MOU sets forth the parameters for WestEd's conduct of the SST Pilot Study and the collection of education record data in the District. This is a non-financial agreement.

1. The Study

The Study, which is funded by the U.S. Department of Education (Institute of Education Sciences [IES], Award No. R305A180224), and led by WestEd, is designed to investigate the effectiveness of *Adventures Aboard the S.S. GRIN*. *S.S. GRIN* is designed to translate the content and cognitive-behavioral strategies of an established, evidence-based social skills training ("SST") program into a game-based virtual world. The program aims to build students' social emotional skills and improve peer relationships for elementary students experiencing a wide range of social difficulties, including peer rejection, bullying, and social anxiety. In order to understand the impact of this SST program on students, researchers will be collecting student data across the entire SST program and will perform observations at selected participating school sites.

The District's participation is dependent upon its willingness and ability to provide the time, space, and data specified below. The District is authorized to release the Data without written parental consent only in accordance with designated, applicable FERPA exceptions in Section 99.30 of Title 34 of the Code of Federal Regulations.

WestEd anticipates that the District's direct costs will be minimal and will not exceed that which is necessary for intervention implementation, data extraction and electronic data transfer to WestEd.

2. Term and Termination

- A. This MOU is effective as of the date first written above and expires June 30, 2019.
- B. Either party may terminate this MOU upon 30 days prior written notice to the other party.

- C. The termination or expiration of this MOU shall not affect the District's rights and WestEd's obligations regarding confidentiality or the retention, storage, or destruction of Data, as set forth herein. Such rights and obligations shall survive the term of this MOU.

3. Definitions

- A. "Data" as used in this MOU refers to the following:

Student-level variables retrieved from the District - the variables below will be requested for individual students participating in the SST Pilot Study.

- Student name and school ID number
 - Grade level
 - Gender
 - Scores on the CELDT as applicable
 - English Learner status
- B. "Personally Identifiable Information" or "PII" as used in this MOU shall mean any information or data that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- C. "De-identified Data", as used in this MOU, shall mean Data from which all Personally Identifiable Information has been removed or obscured so that a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, would not be able to identify any individual student with reasonable certainty.

4. Confidentiality

- A. WestEd shall help ensure any Data available can only be viewed or accessed by agencies legally allowed to do so, in compliance with an applicable Family Educational Rights and Privacy Act exception, and as agreed upon by District and WestEd. Except as otherwise permitted by the terms of this MOU, WestEd shall not use the Data supplied to it in an unauthorized manner. Specifically, WestEd shall not sell or release Data, nor enable or permit third parties to engage in targeted advertising to students or to build student profiles unrelated to the purposes contemplated by this MOU. WestEd shall ensure that any third party who is permitted legal access to the Data is aware of the responsibility to take all reasonably possible precautions to safeguard the Data and comply with all applicable Federal, State, or local laws, ordinances, regulations, and directives relating to confidentiality.
- B. WestEd and its contractors agree to take all necessary precautions to safeguard the data and comply with all applicable Federal, State, or local laws, ordinances, regulations, and directives relating to confidentiality. These include, but are not limited to, the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR part 99), the California Information Practices Act (California Civil Code § 1798 et. seq.), and the Privacy Act of 1974, as amended, (5 U.S.C. § 552).

- C. Personally Identifiable Information (PII) will only be used for the SST Pilot Study as identified in this MOU.
- D. PII will only be used for purposes of the Study identified in this MOU. WestEd will limit internal access to PII to individuals working on the Study with legitimate interests in the PII and on a need to know basis, as required in accordance with FERPA.
- E. WestEd will take steps to maintain the confidentiality of PII at all stages of the SST Pilot Study.
- F. No individual shall be identifiable in any reports, publications, or other documents created by WestEd or its contractors with the use of data.
- G. Retain data in a place physically secure from access by unauthorized persons. Paper-based data will be stored in locked file cabinets. WestEd agrees that any computer or server on which electronic data reside will be password protected at all times. When not in immediate use, electronic data will reside in an encrypted remote server, and not on individual computers.
- H. Provide a secure, encrypted transmission method for storing and transferring the data.
- I. WestEd will destroy all PII when it is no longer needed for the SST Pilot Study and, in any event, no later than 60 days after the expiration of this MOU. The parties may amend the MOU to extend the time period if needed; however such amendment must be in accordance with Section 7.A of this MOU.
- J. In accordance with applicable law and the the data sharing policies of WestEd's prime funder, the US Department of Education, de-identified data will be retained by WestEd beyond the conclusion of the SST Pilot Study and the term of this MOU, and may be shared with other researchers in the spirit of stimulating new advances in education research. Such De-identified Data may be shared with third parties only as permitted by state and federal laws governing the confidentiality of student records.
- K. In the event either the District or WestEd becomes aware of unauthorized disclosures of Data or a breach of data storage and security systems, the parties shall notify each other as promptly as possible, but no later than seventy-two (72) hours after such party becomes aware of the unauthorized disclosure or breach. In the event that such disclosure or breach occurs due to the actions or inactions of WestEd or its employees, agents, and contractors, or while the Data is being stored or used by WestEd or its employees, agents, and contractors, WestEd shall be responsible for taking all measures necessary to determine the scope of the breach and notify all impacted parties, including District students and parents, at the direction and discretion of the District, to the extent required by California Civil Code §1798.29.

5. WestEd's Additional Responsibilities

WestEd shall:

- A. Provide dedicated contact information for this research project. WestEd's contact information is:
Kylie Flynn
Senior Research Associate, STEM Program
WestEd
2470 Mariner Square Loop, Office 257
Alameda, CA 94501
Email: kflynn2@wested.org
Phone: 510-302-4282
- B. Inform parents of students eligible for participation in the SST Pilot Study, and obtain their written permission for their student's participation.
- C. Provide all participating control teachers at Ledesma Elementary School with an honorarium of \$600 for their time in completing behavior rating scales for participating students during the 2018-2019 school year.
- D. Provide all participating teachers (treatment and control) in the pull-out model of implementation at Anderson Elementary school with an honorarium of \$600 for their time in completing behavior rating scales for participating students during the 2018-2019 school year.
- E. Provide participating counselors, or other designated staff, with an honorarium of \$600 for their participation in monitoring students' use of the S.S.GRIN platform during the 2018-2019 school year using the pull-out model of implementation at Anderson Elementary school.
- F. Provide all participating treatment teachers who are part of the in-class implementation model at Stipe Elementary School with an honorarium of \$1200 for their participation in monitoring students' use of the S.S.GRIN platform during the 2018-2019 school year, as well as for their time in completing behavior rating scales for participating students during the 2018-2019 school year.
- G. Provide advance notice of all school visits and interviews and comply with all district and site visit policies.
- H. Provide participating counselors, or other designated staff, online professional development and access to SST curriculum and resources free of cost during the SST Study. Training and access to the SST curriculum and resources for up to 1 year will be provided to the participating teachers, or other designated staff, after the study is completed if the district chooses.

6. District's Additional Responsibilities

The District shall:

- A. Designate a contact person to facilitate communications between the District and WestEd for coordinating the data transfer activities necessary to carry out this MOU. The District contact person is:
- Name: _____
- Title: _____
- Email: _____
- Phone: _____
- B. Collaborate with WestEd in the recruitment of 3rd grade teachers for the SST Pilot Study, and in securing the cooperation of principals for the study to take place at their school.
- C. Allow participating 3rd grade teachers to provide class rosters and screening information on the social skills of their students. WestEd will use this information to select approximately 8 students at each participating school site for inclusion in the study.
- D. For the pull-out model at Anderson Elementary, identify a district employee (e.g., counselor, interventionist, resource specialist, instructional assistant) who could supervise small groups (2-4) of participating treatment students' use of the S.S.GRIN platform. Students will use S.S.GRIN once per week for approximately 45 minutes, for 12 weeks.
- E. For the pull-out model at Anderson Elementary, provide a space outside of the classroom for the intervention to take place with small group(s) of students during the 12-week intervention period.
- F. For the in-class model at Stipe Elementary, allow participating 3rd grade teachers to implement the S.S.GRIN platform in their classroom, either using a class-wide implementation or with participating students only (depending on the school's preference). Students will use S.S.GRIN once per week for approximately 45 minutes, for 12 weeks.
- G. Allow teachers, and other designated staff, to participate in the SST Pilot Study and in the SST online training sessions.
- H. Allow teachers to complete pre- and post- student rating scales on all participating children.
- I. Allow WestEd researchers to observe at selected school sites for the SST Pilot Study.
- J. Provide WestEd with a written copy of all District policies with which WestEd is required to comply.
- K. Collaborate with WestEd, as needed, to facilitate the coordination of the data transfer.

- L. Agree to participate in data sharing for the entire SST Pilot Study, pursuant to the applicable data sharing terms and conditions.
- M. Provide demographic and other information for data gathering, including access to student assessment data for all participating students, pursuant to the applicable data sharing terms and conditions.

7. General Provisions

- A. Amendments. This MOU may be amended at any time by the mutual written agreement of the Parties.
- B. Assignment. Neither Party shall voluntarily or by operation of law, assign or otherwise transfer its rights or obligations under this MOU without the other party's prior written consent. Any purported assignment in violation of this paragraph shall be void.
- C. Severability. The provisions of this MOU are severable and the unenforceability of any provision of this MOU shall not affect the enforceability of any other provisions hereof.
- D. Limitation of Liability. Each Party agrees to indemnify the other against any and all liability, actions, claims, damages, losses, costs, and expenses (including attorneys' fees) arising out of or in any way resulting from the indemnifying Party's own negligent or intentional acts, errors, or omissions in connection to the performance of the responsibilities of each Party, per this MOU.
- E. Relationship Between the Parties. Nothing in this MOU shall be construed to grant either Party the right to make commitments of any kind for or on behalf of the other Party, without the prior written consent of the other Party. Nothing in this MOU shall be deemed to constitute, create, give effect to, or otherwise recognize an employment relationship between the parties or a joint venture, partnership, or formal entity of any kind.
- F. Dispute Resolution. The Parties shall exercise their best good faith efforts to settle any claim, controversy, or dispute (individually or jointly, a "Dispute") arising out of or relating to this MOU. Representatives of the Parties shall discuss any Dispute no later than fifteen (15) days after either Party gives written notice to the other Party of a Dispute. Such notice will include the legal and factual basis for such Dispute. No arbitration or other dispute resolution proceeding may be commenced before representatives of the Parties have met pursuant to this provision. In the event that a Dispute cannot be resolved through good faith negotiations, the Parties agree that such Dispute shall be finally settled through binding arbitration. The arbitration shall be administered by Judicial Arbitration and Mediation Services, Inc. ("JAMS"), located in San Francisco, California, pursuant to its Comprehensive Arbitration Rules and Procedures. The Parties agree that the decision of the JAMS arbitrator shall be final and conclusive upon the Parties. Judgment on the award rendered by the JAMS arbitrator may be entered in any court having jurisdiction. Notwithstanding the foregoing, either Party may seek injunctive or provisional relief to protect confidential information at any time and need not proceed with alternative dispute resolution before seeking such relief.

G. Execution. Each of the persons signing this MOU represents that he or she has the authority to sign on behalf of and bind their respective Party.

H. Entire Agreement. This MOU is the entire agreement between the parties. No other agreements, oral or written, have been entered into with respect to the subject matter of this MOU.

IN WITNESS WHEREOF, the parties have, by their respective duly authorized representatives, executed this MOU as of the day and year first written above.

WestEd

By:

Name: Mike Newenfeldt

Title: Deputy CFO

Date:

3/15/19

Oak Grove School District

By:

Name:

Title:

Date:

Please return this form via e-mail to kflynn2@wested.org

EXHIBIT "B"
SCHEDULE OF DATA

| Category of Data | Element | 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 | X |
| | Observation data | X |
| | 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 | X |
| Demographics | Date of Birth | |
| | Place of Birth | |
| | Gender | X |
| | Ethnicity or race | X |
| | Language information (native, preferred or primary language spoken by student) | X |
| | Other demographic information-Please specify: | |
| Enrollment | Student school enrollment | X |
| | Student grade level | X |
| | Honors | |
| | Guidance counselor | |
| | Specific curriculum program | X |
| | 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 | X |
| | Low income status | X |
| | Medical alerts/health data | |

| | | |
|-----------------------------|--|---|
| | Student disability information | |
| | Specialized education services (IEP or 504) | X |
| | 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

_____ directs **WestEd** 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:

| | |
|--|---|
| Extent of Disposition 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. |
| Nature of Disposition Disposition shall be by: | <input type="checkbox"/> Destruction or deletion of data. <input checked="" 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. |
| Timing of Disposition 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>6/30/2029</u> |

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

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 02/27/2019 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: **WestEd**

BY: 

Date: **03/15/2019**

Printed Name: **Mike Neuenfeldt**

Title/Position: **Deputy CEO**

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: **Mike Neuenfeldt**

Title: **Deputy CEO**

Email Address: **contracts@wested.org**

EXHIBIT "F" DATA SECURITY REQUIREMENTS

00618-00001-0274378.1