

**CALIFORNIA STUDENT DATA PRIVACY
AGREEMENT Version 2.0 (September 26, 2018)**

**School District/Local Education Agency:
Lodi Unified School District**

AND

**Provider:
WestEd**

Date: 1/10/2019

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the
Lodi Unified School District

(hereinafter referred to as “LEA”) and WestEd, a California joint powers agency
(hereinafter referred to as “Provider”) on January 10, 2019 . The Parties agree to
the terms as stated herein.

RECITALS

WHEREAS, the Local Education Agency (“LEA”) has agreed to participate in an evaluation of an online education platform that hosts national engineering design and innovation challenges for K-12 students, funded by the U.S. Department of Education, Institute of Education Sciences (the “Study”) pursuant to a memorandum of understanding dated (“Service Agreement”); and

WHEREAS, in order to participate in the Study 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 in connection with the Study may also be 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 DP A, 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, which may include the FERPA, PPRA, COPPA, SOPIPA, AB1584, 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 Parties have agreed to engage in certain activities in connection with the Study, as further outlined in Exhibit "A" hereto:

See Exhibit A - Memorandum of Agreement for the Future Engineers Study

- 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 submit to criminal background checks if required by state law or 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 the Study or 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 **initial** 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 or required by law. 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 caused by Processor or Processor's contractor, processor, or agent.
- 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 below:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Leonard Kahn

Title: Chief Business Officer

Contact Information:

LKahn@lodiUSD.net

The designated representative for the Provider for this Agreement is:

Name: Mike Neuenfeldt

Title: Deputy CFO

Contact Information:

WestEd Contracts Management Department

730 Harrison Street, 5th Floor

San Francisco, CA 94107

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 CFO

Contact Information:

WestEd Contracts Management Dept.

6. Entire Agreement. This DPA, together with the Service Agreement, 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 DP A may be amended and the observance of any provision of this DP A may be waived (either generally or in any particular instance and

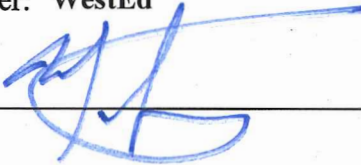
either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, 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

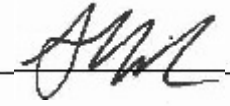
BY:  Date: 1.10.19

Printed Name: Mike Neuenfeldt Title/Position: Deputy CFO

Local Education Agency: Lodi Unified School District

EAH
2/7/19

BY: Leonard Kahn Date: 1/17/19

Printed Name:  Title/Position: Chief Business Officer

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

SEE ATTACHED MOU.

MEMORANDUM OF UNDERSTANDING
Lodi Unified School District and WestEd
for the Future Engineers Study

This Memorandum of Understanding (“MOU”) outlines the agreement by and between WestEd and Lodi Unified School District (the “Program”) to conduct the Future Engineers Study (the “Study”) funded by the U.S. Department of Education and is entered into on January 10, 2019.

1. Purpose

Future Engineers is developing an online education platform that hosts national engineering design and innovation challenges for K-12 students. All challenges are offered free for student and classroom participation and are aligned with STEAM and Maker education. The purpose of the study is to explore how teachers’ and students’ participation in Future Engineers design challenges helps support middle school students’ understanding of science and engineering practices. The Study will take place over the course of nine months, from September 2018 – May 2019. Teacher and student participation is voluntary.

Participating teachers will be **randomly assigned** to either the *treatment group* (which will use the Future Engineers website in the Fall 2018 semester) or the *control group* (which have the option of using the Future Engineers website after the completion of the study).

This MOU sets forth the agreement between the Program and WestEd regarding the Program’s role in the Study. This is a non-financial agreement.

2. Definitions

- A. "Data" as used in this MOU shall mean any data collected from teachers or students, including but not limited to student demographic data, including age, race, gender, and preferred home language, student survey data, student assessment data, and teacher interview data that will be collected as part of the Study.
- 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 or teacher that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student or teacher with reasonable certainty.
- C. "De-identified Data" as used in this MOU shall mean Data from which enough Personally Identifiable Information has been removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the remaining information can be used to identify an individual.

3. Term and Termination

- A. This MOU is effective as of the last signature date of the parties.
- B. This MOU expires on December 31, 2019.
- C. Either party may terminate this MOU prior to December 31, 2019, without cause, provided that written notice is given at least 45 days in advance of termination.

4. Confidentiality

- A. 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).
- B. Data containing Personally Identifiable Information will only be used for the Study identified in this MOU.
- C. WestEd will limit access to PII to only those individuals working on the Study who have legitimate interests in the PII and on a need to know basis.
- D. WestEd will take steps to maintain the confidentiality of all PII at all stages of the Study, and use only secure, encrypted methods of transmission and ensure that any computer on which PII is stored is encrypted.
- E. No individual shall be identifiable in any reports, publications, or other documents created by WestEd or its contractors with the use of Data.
- F. WestEd will destroy all PII when it is no longer needed for the Study and no later than 60 days after the expiration date 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.

5. WestEd Responsibilities

WestEd shall:

- A. Designate a contact person for this research project. WestEd's contact person is:

Michelle Tiu	WestEd
Senior Research Associate	300 Unicorn Park Drive
	5 th Floor
	Woburn, MA 01801
	Telephone: (781) 481-1129
	Email: mtiu@wested.org
- B. Collect all Data directly from Program teachers and students during the Study. Use the Data collected for research purposes only. Retain all Data in a place physically secure from access by unauthorized persons. Any computer on which the Data reside will be password protected at all times.
- C. Keep the Program informed of all major Study activities, including providing teachers with advances notice of all student assessments, classroom observations, and teacher interviews.
- D. Provide Program with an informational letter and consent form for the Study, which Program will in turn distribute to students and parents of participating students.
- E. For each selected participating teacher, conduct one observation in the teacher's classroom during the Study. (Not all teachers will be selected for an observation.)
- F. For each selected participating teacher, conduct a 60-minute interview with the teacher at the end of the Study. (Not all teachers will be selected for an interview.)

In addition to the items listed in 5.A through 5.F above, for each participating teacher selected for the Treatment Group, WestEd shall:

- G. Provide access to the Future Engineers website for use by participating students and teachers during the Study.
- H. Provide each participating teacher with a stipend totaling \$800 upon completion of all required Study activities. Stipends shall be paid no later than 30 days following the end date of the Study.

In addition to the items listed in 5.A through 5.F above, for each participating teacher selected for the Control Group, WestEd shall:

- I. Provide participating teachers with access to the Future Engineers website at the end of the Study.
- J. Provide each participating teacher with a stipend totaling \$500 upon completion of all required Study activities. Stipends shall be paid no later than 30 days following the end date of the Study.

6. Program Responsibilities

The Program shall:

- A. Designate a contact person for this research project. The Program's contact person is:
Name and Title: _____
Mailing Address: _____
Telephone: _____
Email: _____
- B. Collaborate with WestEd, as needed, to facilitate the coordination of the research activities, including any required permissions activities related to the Study.

The Program's participating teachers shall:

- C. Agree to be randomly assigned into either the treatment group or control group.
- D. Teach one middle school (Grades 6-8) science or engineering class during the 2018-19 school year. The class must be a year-long (and not semester-long) class.
- E. Teach the following two science and engineering topics during the 2018-19 school year:
 - a. Weather, for at least 6 weeks during the fall semester
 - b. Light waves, for at least 2 weeks during the spring semester
- F. Distribute and collect informational letters and opt out forms from parents and students in their science or engineering class.
- G. Complete a 10-minute teacher background survey.
- H. Facilitate the administration of student pre- and post-assessments and pre- and post-surveys during the Study.
- I. Complete weekly online teacher logs during the weeks their classes are participating in design challenges during the Study (for treatment teachers) or learning content covered in the design challenges (for control teachers).

- J. Provide students with regular access to Internet-enabled computers in order to complete study activities. Provide students with access to a camera to take photos and videos of their designs twice during the Study.
- K. Facilitate student access to found/recycled household materials such as: fasteners, adhesives, scissors, pennies, flashlights, string, water, etc.

In addition to the items 6.C through 6.K, above, all participating teachers selected for the Treatment Group shall:

- L. Participate in a 90-minute online orientation at the beginning of the Study to introduce them to the Future Engineers online platform and to review the study requirements.
- M. Incorporate three Future Engineers design challenges into their instruction over the course of the study from September 2018 – May 2019. The challenges will be comprised of two pre-identified topics (weather, light waves) and one topic of the teacher's choice.
- N. Complete a pre- and post-implementation teacher survey.
- O. If selected, allow one WestEd researcher to conduct a classroom observation during the Study.
- P. If selected, participate in a 1-hour interview with a WestEd researcher at the end of the Study.

In addition to the items 6.C through 6.K, above, all participating teachers selected for the Control Group shall:

- Q. Participate in a 45-minute online orientation at the beginning of the Study to review the study requirements.
- R. Agree to *not* use the Future Engineers design challenges or any aspect of the Future Engineers website during the Study, and agree to conduct classroom activities "as usual" during the Study period. *(Teachers assigned to the control group will receive access to use Future Engineers design challenges in their classrooms after the study has been completed.)*

7. General Terms

- A. Amendments. This MOU may be amended at any time by mutual agreement of the parties without additional consideration, provided that before any amendment shall take effect, it shall be in writing and signed by both 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. Dispute Resolution. The parties will attempt to settle any dispute, claim or controversy arising out of or relating to this MOU, including the breach, enforcement, interpretation or validity thereof ("Dispute" or "Disputes") through good faith negotiations. Such negotiations shall take place face to face, between representatives authorized to settle the Dispute, within 30 days from the date one party provides the other party with written notice of a Dispute and the legal and factual basis for such Dispute ("Negotiations"). The parties agree to final settlement by arbitration of any Dispute that cannot be resolved through good faith Negotiations. No party shall submit an arbitration

demand or complaint until the parties have engaged in Negotiations and those Negotiations have ended in an impasse. The arbitration of Disputes shall be administered by JAMS in San Francisco, California, pursuant to its Comprehensive Arbitration Rules and Procedures. Judgment on the award rendered by the arbitrators may be entered in any court having jurisdiction. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction. Notwithstanding the foregoing, no Dispute concerning a party's or a third party's rights in or to intellectual property protected in accordance with Federal law (an "IP Dispute") shall be subject to arbitration and any such IP Dispute may be filed only in a federal court of competent jurisdiction, subject to the obligation to participate in Negotiations, as set forth herein.

- E. 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. This Agreement may be executed in two or more counterparts, each of which together shall be deemed to be an original, but all of which, taken together, shall constitute one and the same Agreement.
- F. Entire Agreement. This MOU is the entire agreement between the parties. All prior agreements or understandings, oral or written, between the parties relating to the subject of this MOU are superseded by this MOU. This Agreement may only be modified or amended by a writing signed by both parties. Both parties explicitly acknowledge and agree that any subsequent oral agreements, oral understandings, and oral proposals are null and void.

In witness whereof, this Memorandum of Understanding has been executed by the parties hereto.

WestEd

Signature: _____

Printed Name: Michael J. Neuenfeldt

Title: Deputy CFO

Date: 1.10.19

Lodi Unified School District

Signature: _____

Printed Name: _____

Title: _____

Date: _____

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used in the Study
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	X
	Other assessment data-Please specify:	X - Student science assessment (researcher-developed measure used only for study purposes)
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	X - as self-reported by students, not collected from the district
	Ethnicity or race	X - as self-reported by students, not collected from the district
	Language information (native, preferred or primary language spoken by student)	X - as self-reported by students, not collected from the district
Enrollment	Other demographic information- Please specify:	
	Student school enrollment	
	Student grade level	X - as self-reported by students, not collected from the district
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Other enrollment information- Please specify:		
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
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)	X - as self-reported by students, not collected from the district
	Living situations (homeless/ foster care)	
	Other indicator information- Please specify:	X - Free and Reduced Lunch eligibility, as self- reported by students, not collected from the district
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID	

	number	
	State ID number	
	Provider/App assigned student ID number	X - Students will be provided with an ID number for the study, so that all student names can be removed and data can be deidentified
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X - data will be deidentified
Student In App Performance	Program/appli- cation 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	x
Student work	Student generated content; writing, pictures etc.	x
	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 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 needed.

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identified 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 DP A, 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," to the extent that provider engages in any of the activities described in this definition. 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 DP A 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. The term "pupil-generated content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

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. Pupil Records does not include any of the categories of information excluded from the definition of “Pupil records“ under Cal. Ed. Code section 49073.1.

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 SO PIP A 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:

<u>Extent of Disposition</u> Disposition shall be:	<input type="checkbox"/> Partial. The categories of data to be disposed of are as follows: <input type="checkbox"/> Complete. Disposition extends to all categories of data.
<u>Nature of Disposition</u> Disposition shall be by:	<input 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 type="checkbox"/> By (Insert Date) _____

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "F" DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]