Contract No. 20-457

DATA PRIVACY AMENDMENT TO AGREEMENT
THE PLEASANTON UNIFIED SCHOOL DISTRICT

AND

BOARD APPROVED
DATE 4/21/2020

ASSISTments

WHEREAS, the Pleasanton Unified School District ("District") and [ASSISTments], (hereinafter referred to as Provider"), have entered into an Agreement whereby Provider has agreed to provide [support for homework in math, ASSISTments assists students while helping teachers assess where to focus instructional time in mathematics.]; (hereinafter referred to as "Service") and

WHEREAS, in order to provide the Services described above, Provider may receive documents defined as student records under FERPA and California AB 1584, among other statutes, which are therefore subject to statutory protection; and

WHEREAS, the Agreement, either having been executed prior to or after the enactment of AB 1584, (currently found in Education Code section 49073.1), and may not contain all of the provisions required by that Statute;

WHEREAS, the parties wish to execute this Amendment to bring the underlying Agreement in full compliance with AB 1584.

NOW THEREFORE, for good and valuable consideration, the Parties agrees as follows:

PURPOSE

1. The purpose of this Amendment is to bind the parties to uphold their responsibilities under all applicable privacy statutes, including the Family Education Rights Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and AB 1584, found in Education Code including Section 49073.1). Specific duties are set forth below.

DATA OWNERSHIP AND AUTHORIZED ACCESS

2. Data Property of District: All information, data, and other content transmitted by the District to the Provider, or entered or uploaded under District's user accounts, remain the sole property of the District. The District retains exclusive control over student and staff data, including determining who may access data and how it may be used for legitimate authorized purposes. Provider and the District shall establish reasonable procedures by which a parent, legal guardian or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account. [See attached security guidelines]

3. Data Access: Provider may access District data solely to fulfill its obligations under this Amendment.

4. Third Party Access: Provider may not distribute District data or content to a third party without District's express written consent, unless required by law. Use of subcontractors and subcontractor access

to data must be approved in writing by the District. Provider will ensure that approved subcontractors adhere to all provisions of the Agreement and this Amendment.

5. Third Party Request: Should a third party contact Provider with a request for District data, including law enforcement and government entities, the Provider shall redirect the third party to request the data directly from the District. Provider shall notify the District in advance of a compelled disclosure to a third party unless legally prohibited.

6. Applicability of COPPA: Provider warrants to District that all data collected directly from children and/or data resulting from tracking children's use of the service is subject to parental consent and will occur in strict conformity to the requirements of the Children's Online Privacy Protection Act (COPPA). Provider shall obtain such parental consent, unless expressly agreed to otherwise by the parties. Provider may not sell or market student data, or use student data for sale or marketing purposes without express parental consent.

DUTIES

7. District: The District will perform the following duties:

(a) Provide Data: Provide data for the purposes of the Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g.

(b) Precautions: Take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

(c) Notification: Notify Provider promptly of any known or suspected unauthorized access.

8. Provider: Provider will perform the following duties:

(a) Privacy Compliance: Comply with all FERPA, COPPA, PPRA and AB 1584 (Education Code section 49073.1), among others. These duties shall include the following:

(b) Authorized Use: The data shared under the Agreement shall be used for no purpose other than the work stated in this Amendment and or otherwise authorized under the statutes referred to in subsection (a), above.

(c) Employees Bound: Require all employees of Provider and agents of any kind to comply with all applicable provisions of FERPA laws with respect to the data shared under this Amendment. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to data pursuant to this Amendment.

(d) Secure Environment: Maintain all data obtained pursuant to this Amendment in a secure computer environment and not copy, reproduce or transmit data obtained pursuant to this Amendment except as necessary to fulfill the purpose of the original request. Provider has security measures in place to help protect against loss, misuse and alteration of the data under Provider's control. When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology protects information, using both server authentication

and data encryption to help ensure that data are safe, secure and available to only authorized users. Provider shall host the service in a secure server environment that uses a firewall and other advance technology in an effort to prevent interference or access from outside intruders. The service will require unique account identifiers, usernames and passwords that must be entered each time a client or user signs on.

(e) No Disclosure: Not disclose any data obtained under this Amendment in a manner that could identify an individual student to any other entity in published results of studies as authorized by this Amendment. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services or applications.

(f) Disposition of Data: Destroy all personally identifiable data obtained under this Amendment when it is no longer needed for the purpose for which it was obtained, or transfer said data to the District or District's designee, according to a schedule and procedure as the Parties may reasonable agree. Nothing in this Amendment authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

(g) Data Breach Notification: Upon becoming aware of any unlawful or unauthorized access to District data stored on equipment used by Provider or in facilities used by Provider, Provider will: promptly notify the District of the suspected or actual incident; promptly investigate the incident and provide District with detailed information regarding the incident, including the identity of affected users; support the District in its efforts to notify affected users; pay for usual and reasonable costs; and use reasonable steps to mitigate the effects and to minimize any damage resulting from the incident.

DATA REQUEST - N/A

9. Data Requested: [Describe the data that will be shared with the Provider and/or entered directly by PUSD staff or student.]

10. School Year: Provider is requesting data for the following school year(s): ~~July 1,~~ 4/6/2020 through June 30, 2020.

AUDIT

11. The District reserves the right to audit and inspect the Provider's compliance with this Amendment and applicable law.

AGREEMENT

12. Priority of Agreements: This Amendment shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of this Amendment and the Agreement or any other bid/RFP, license agreement, or contract document(s) in existence, the terms of this Amendment shall apply.

13. Other Provisions Unaffected: Except as described in paragraph 12 above, all other provisions of the Agreement shall remain unaffected.

14. Modification of Agreement: No modification or waiver of any term of this Amendment is effective unless both parties sign it.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the last day noted below.

PLEASANTON UNIFIED SCHOOL DISTRICT

By: Janet Wolfinger Date: 4/6/2020

Printed Name: JWolfinger Title/Position: Coordinator Purchasing, Warehouse & Graphics

Provider Legal Name ASSISTments

By: Neil T. Heffernan Date: April 2, 2020

Printed Name: Neil T. Heffernan Title/Position: WPI professor Founder of ASSISTments

Note: Electronic signature not permitted.

REV May 2017

REV May 2017

ASSISTments

This Security Guidelines document sets forth the duties and obligations of ASSISTments (defined below) with respect to Personally Identifiable Information (defined below). In the event of any inconsistencies between the DPSG and the Agreement (defined below), the parties agree that the DPSG will supersede and prevail. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions.
    1. **"Agreement"** means the Agreement between ASSISTments and Subscriber to which these Security Guidelines are referenced and made a part thereof.
    2. **"Applicable Laws"** means federal, state and international privacy, data protection and information security-related laws, rules and regulations applicable to the Services and to Personally Identifiable Information.
    3. **"End User Data"** means the data provided to or collected by ASSISTments in connection with ASSISTments's obligations to provide the Services under the Agreement.
    4. **"Personally Identifiable Information"** or **"PII"** means information provided to ASSISTments in connection with ASSISTments's obligations to provide the Services under the Agreement that (i) could reasonably identify the individual to whom such information pertains or (ii) can be used to authenticate that individual, such as passwords, unique identification numbers or (iii) is protected under Applicable Laws. For the avoidance of doubt, PII does not include aggregate, anonymized data derived from an identified or identifiable individual.
    5. **"Processing of PII"** means any operation or set of operations which is performed upon PII, such as collection, recording, organization, storage, use, retrieval, transmission, erasure or destruction.
    6. **"Security Incident"** means the unlawful access to, acquisition of, disclosure of, loss, or use of PII.
    7. **"Services"** means any services and/or products provided by ASSISTments in accordance with the Agreement.

2. Confidentiality and Non-Use; Consents.
    1. ASSISTments agrees that the PII is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement, ASSISTments shall not Process PII for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.

2. ASSISTments shall maintain PII confidential, in accordance with the terms set forth in this Security Guidelines and Applicable Laws. ASSISTments shall require all of its employees authorized by ASSISTments to access PII and all Third Parties to comply with (i) limitations consistent with the foregoing, and (ii) all Applicable Laws.
3. Subscriber represents and warrants that in connection with any PII provided directly by Subscriber to ASSISTments, Subscriber shall be solely responsible for (i) notifying End Users that ASSISTments will Process their PII in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.

3. Data Security.

ASSISTments shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of PII. ASSISTments's security measures include the following:

1. Access to PII is restricted solely to ASSISTments's staff who need such access to carry out the responsibilities of ASSISTments under the Agreement.
2. Access to computer applications and PII are managed through appropriate user ID/password procedures.
3. Access to PII is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such PII).
4. Data is encrypted in transmission (including via web interface) at no less than 128-bit level encryption.

4. Data Security Breach

1. In the event of a Security Incident, ASSISTments shall (i) investigate the Security Incident, identify the impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to Subscriber or individuals affected by the Security Incident that ASSISTments is required by law, subject to applicable confidentiality obligations and to the extent allowed and/or required by and not prohibited by Applicable Laws or law enforcement.
2. Except to the extent prohibited by Applicable Laws or law enforcement, ASSISTments shall, upon Subscriber's written request, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

5. Security Questionnaire.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, ASSISTments shall respond to security questionnaires provided by Subscriber, with regard to ASSISTments's information security program applicable to the Services, provided that such information is available in the ordinary course of business for ASSISTments and it is not subject to any restrictions pursuant to ASSISTments's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise ASSISTments's confidentiality obligations and/or legal obligations or privileges. Additionally, in no event shall ASSISTments be required to make any disclosures prohibited by Applicable Laws. All the information provided to Subscriber under this section shall be Confidential Information of ASSISTments and shall be treated as such by the Subscriber.

6. Security Audit.

Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, ASSISTments's data security measures may be reviewed by Subscriber through an informal audit of policies and procedures or through an independent auditor's inspection of security methods used within ASSISTments's infrastructure, storage, and other physical security, any such audit to be at Subscriber's sole expense and subject to a mutually agreeable confidentiality agreement and at mutually agreeable timing, or, alternatively, ASSISTments may provide Subscriber with a copy of any third party audit that ASSISTments may have commissioned.

7. Records Retention and Disposal.

1. ASSISTments will use commercially reasonable efforts to retain End User Data.
2. ASSISTments will use commercially reasonable efforts to regularly back up the Subscriber and End User Data and retain any such backup copies for a minimum of 12 months.