

**DATA PRIVACY AMENDMENT TO AGREEMENT  
THE PLEASANTON UNIFIED SCHOOL DISTRICT**

**AND**

IXL Learning, Inc.

**WHEREAS**, the Pleasanton Unified School District ("District") and IXL Learning, Inc., (hereinafter referred to as Provider"), have entered into an Agreement whereby Provider has agreed to provide IXL Learning Services; (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. Upon request from the District, the Provider will update pupil's records.

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. District agrees that Provider may share

District data or portions thereof with Provider's vendors for the purpose of providing the Service, improving the Service, and performing back-office functions relating to the Service, so long as said vendors are contractually obligated to (i) not use any covered information for any purpose other than providing the contracted service to, or on behalf of, IXL, (ii) not disclose any District Data provided by IXL with subsequent third parties, (iii) implement and maintain reasonable security procedures and practices, and (iv) delete or de-identify District Data upon request of the District.

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 ask 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: The District represents that it has the authority to provide District Data to Provider for the purpose of performing its obligations under the Agreement, and that the District has provided appropriate disclosures to students, parents, guardians and other users regarding its sharing of District Data with Contractor. 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 both during and after the term of the Agreement. Provider may use aggregate information derived from District Data for marketing purposes.

(f) Disposition of Data: Destroy or de-identify 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 reasonably agree. Certain residual data may persist in backups that are not used or accessed in the ordinary course of business, and which are overwritten according to the standard retention schedule for backup datasets. To the extent that such backups are restored, the de-identification process(es) shall be re-executed so that such residual data in the restored backup is deleted or destroyed

(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

9. Data Requested: IXL Roster Spreadsheet has been provided (attached) because the District has the option of providing as much or little of the information on the rostering spreadsheet as deemed necessary by the District. The IXL Service may be used on a pseudonymous basis. IXL's Service can be used without PII so we give the customer the option of providing whatever PII they would like.

10. School Year: Provider is requesting data for the following school year(s): July 1, 2019 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. Provider shall be required to comply with the obligations of this section only to the extent that such auditing or inspection activities are mandated by applicable federal or state 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.

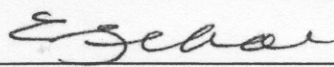
13. Other Provisions Unaffected: Except as described in paragraph 12 above, all other provisions of the Agreement shall remain unaffected.

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

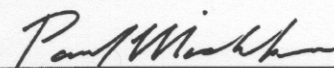
By: 

Date: 7/31/19

Printed Name: Ellen Rebosura

Title/Position: Coordinator of Purchasing

IXL Learning, Inc.

By: 

Date: 8/1/2019

Printed Name: Paul Mishkin

Title/Position: CEO

*Note: Electronic signature not permitted.*