# WISCONSIN STUDENT DATA PRIVACY AGREEMENT
# DISTRICT MODIFIED

School District/Local Education Agency: Cedarburg School District

AND

Provider: IXL Learning, Inc.
Quia Web

Date: 9/8/2023

This Wisconsin Student Data Privacy Agreement – District Modified ("DPA") is entered into by and between the Cedarburg School District (hereinafter referred to as "LEA") and IXL (hereinafter referred to as "Provider") as of August 17, 2023. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS,** the Provider agrees to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to the IXL Learning Terms of Service (available at www.ixl.com/termsofservice) ("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 and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; and 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 Wisconsin state student privacy laws, including pupil records law under Wis. Stat. § 118.125 and notice requirements for the unauthorized acquisition of personal information under Wis. Stat. § 134.98; and

**WHEREAS**, for the purposes of this DPA, Provider is a school district 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 Wisconsin 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 including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and applicable Wisconsin law, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School District 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 further outlined in Exhibit "A" hereto:

IXL Site Licenses (Grades K-12); subjects Math, ELA, Science and Social Studies

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".

***Note:*** *Include only the data elements necessary to perform the Services to LEA*

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 terms used in the Service Agreement, or any other document, including but not limited to Provider's Terms of Use or Service, Privacy Policies, etc.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to or collected by 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 DPA 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 District 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 30 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 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 Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the Student Data directly from the LEA. Provider shall notify the LEA as soon as possible 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 a manner consistent with the terms of this DPA, as well as state and federal law.

## ARTICLE III: DUTIES OF LEA

**1.** **Privacy Compliance**. LEA shall provide Student Data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable Wisconsin law.

**2.** **Annual Notification of Rights**. The LEA shall include a specification of criteria under FERPA 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 Student 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 Student Data privacy and security, including FERPA, COPPA, PPRA, and applicable Wisconsin law.

**2.** **Authorized Use**. The Student 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 outlined in Exhibit A 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. Provider may use De-Identified Data (as that term is defined in this DPA) only for the purposes set forth in this DPA.

**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 Student

Data shared under the Service Agreement.

**4.** **No Disclosure**. Provider shall not copy, reproduce or transmit any Student Data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

**5.** **De-Identified Data**. Upon approval by LEA of Provider's de-identification methodology (see Ex. G), Provider may de-identify Student Data and use that De-Identified Data for the following purposes only: (1) assisting the LEA or other government agencies in conducting research and other studies; (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purposes and for customized student learning. Provider agrees not to attempt to re- identify that De-Identified Data. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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 the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

6. **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 Student 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 written request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data within thirty (30) 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 the Student Data shall be subject to LEA's request to transfer such 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 and receipt of written request from LEA, Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the Student Data, Provider shall notify LEA in writing of its option to transfer such data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of the Student Data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that such data will not be transferred to a separate account.

7. **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 LEA's 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 shall further detail its security programs and measures in Exhibit "F" hereto, such as Provider's adoption of nationally recognized standards or cybersecurity frameworks." 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 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 upon receipt of written request from LEA 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 6, 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 Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of Student 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 that maintains Student Data.

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 Student Data from unauthorized access. The Service security measures shall include server authentication and Student Data encryption. Provider shall host such 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, including by requiring their employees sign confidentiality agreements regarding Student Data. 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 or as specified in the nationally recognized cybersecurity standard/framework that Provider has adopted as specified in Exhibit F) risk assessments and remediate an identified security and privacy vulnerabilities in a timely manner.

**2.** **<u>Data Storage</u>**. Where required by applicable law, Student Data shall be stored within the United States. Provider shall list in Exhibit F the location(s) where Student Data is stored.

**3.** **<u>Audits</u>**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to inspect and/or audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of Services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

**4.** **<u>Data Breach</u>**. 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 of becoming aware of such an event. 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 because 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 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 written 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 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 Student 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, or any other document, including but not limited to Provider's Terms of Use or Service, Privacy Policies, etc., 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: Kirstin Lindstrom-Collins
Title: Director of Technology
and Assessment

Contact Information:
W68N611 Evergreen Blvd.
Cedarburg, WI 53012

The designated representative for the Provider for this Agreement
is: Name: Contracts Administration
Title: Legal

Contact Information:

777 Mariners Island Blvd., Suite 600
San Mateo, CA 94404
legalnotices@ixl.com

**b. Notification of Acceptance of General Offer of Privacy Terms**. Upon execution of Exhibit "E", General Offer of Privacy 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 notice of acceptance of the General Offer of Privacy Terms is:
Name: Contracts Administration
Title: Legal

Contact Information:
777 Mariners Island Blvd., Suite 600
San Mateo, CA 94404
legalnotices@ixl.com

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 OF WISCONSIN, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION OF THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

**9.** **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, 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..

**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 Provider. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

[*Signature Page Follows*]

**IN WITNESS WHEREOF**, the parties have executed this Wisconsin Student Data Privacy Agreement – District Modified as of the last day noted below.

Provider:

BY:____________________ Date: 9/8/2023

Printed Name: Paul Mishkin Title/Position: Chief Executive Officer

Local Education Agency:

BY:____________________ Date: 9/8/2023

Printed Name: Kirstin Collins Title/Position: Director of Technology

***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]

https://www.ixl.com/
The IXL Service, pursuant to the IXL Terms of Service (www.ixl.com/termsofservice) and IXL Privacy Policy (www.ixl.com/privacypolicy).

https://www.quia.com/web
The Quia Service, pursuant to the Quia Terms of Service,
(https://www.quia.com/web/terms_of_service.html) and the Quia Privacy Policy
(https://www.quia.com/web/privacy_policy.html)

# EXHIBIT "B"

## SCHEDULE OF DATA

| **Category of Data** | **Elements** | **Check if Collected or Generated by System** | **Check if to be Provided by District** |
|---|---|---|---|
| | | | |
| **Application Technology Meta Data** | IP Addresses of users, Use of cookies etc. Please specify: | X | |
| | Other application technology meta data Please specify: | | |
| | | | |
| **Application Use Statistics** | Meta data on user interaction with application | X | |
| | | | |
| **Assessment** | Standardized test scores | | |
| | Observation data | | |
| | Other assessment data Please specify: | | |
| | | | |
| **Attendance** | Student school (daily) attendance data | | |
| | Student class attendance data | | |
| | | | |
| **Communications** | Online communications that are captured (emails, blog entries) | | |
| | | | |
| **Conduct** | Conduct or behavioral data | | |
| | | | |
| **Demographics** | Date of Birth | | |
| | Place of Birth | | |
| | Gender | | |
| | Ethnicity or race | | |
| | Language information (native, preferred or primary language spoken by student) | | |
| | Other demographic information- Please specify: | | |
| | | | |
| **Enrollment** | Student school enrollment | | |
| | Student grade level | | |
| | Homeroom | | |
| | Guidance counselor | | |
| | Specific curriculum 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 | X | |
| | | | |
| **Special Indicator** | English language learner information | | |
| | Low income status | | |
| | Medical alerts /health data | | |
| | Student disability information | | |
| | Specialized education services (IEP or 504) | | |
| | Living situations (homeless/foster care) | | |
| | Other indicator information- Please specify: | | |
| | | | |
| **Student Contact Information** | Address | | |
| | Email | X | |
| | Phone | | |
| | | | |
| **Student Identifiers** | Local (School district) ID number | | X |
| | State ID number | | X |
| | Vendor/App assigned student ID number | X | |
| | Student app username | X | |
| | Student app password | X | |
| | | | |
| **Student Name** | First and/or Last | | X |
| | | | |
| **Student In App Performance** | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)<br>Other student in app performance please specify | X | |

| | | | |
|---|---|---|---|
| | | | |
| **Student Program** | Academic or extracurricular activities a student may belong to or participate in | | |

| | | | |
|---|---|---|---|
| **Membership** | | | |
| | | | |
| **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 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

Please see https://www.ixl.com/privacypolicy/serviceprivacypolicy for data types collected.

## EXHIBIT "C"

DEFINITIONS

**De-Identified Data and De-Identification**: Records and information are considered to be De-Identified when all personally identifiable information (including direct and indirect identifiers) has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the LEA, or Provider (upon approval by the LEA of the Provider's de-identification methodology), has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, taking into account other reasonably available information.

**Educational Records**: Educational Records are records, files, other materials and data directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

**Metadata**: means information that provides meaning and context to other data being collected, including but not limited to: date and time records and purpose of creation.

**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 and DPA, 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 DPA, 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 all of the following: (1) Any information that directly relates to a pupil that is maintained by LEA; (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; and any information that meets the definition of a "pupil record" under Wis. Stat. § 118.125(1)(d). For the purposes of this DPA, 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 DPA.

**Service Agreement**: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

**School District Official**: For the purposes of this DPA and pursuant to 34 CFR 99.31 (b) and Wis. Stat. § 118.125(2)(d), a School District 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) and Wis. Stat. § 118.125(2) governing the use and re-disclosure of personally identifiable information from education records.

**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 Wisconsin 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 DPA, 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 DPA, 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

[Name or District or LEA] directs [Name of Provider] 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**<br>Disposition shall be: | _____Partial. The categories of data to be disposed of are as follows:<br>_____Complete. Disposition extends to all categories of data. |
| | |
| **Nature of Disposition**<br>Disposition shall be by: | _____Destruction or deletion of data.<br>_____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**<br>Data shall be disposed of by the following date: | _____As soon as commercially practicable<br>By (Insert Date) ___________________________<br>[Insert or attach special instructions] |

Authorized Representative of LEA

. Dat

e Verification of Disposition of Data

Date by Authorized Representative of Provider

. .

## EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
CEDARBURG SCHOOL DISTRICT

### 1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Cedarburg School District and which is dated to any other LEA ("Subscribing LEA") who accepts this General Offer though 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:

Date: 9/8/2023

BY:

Printed Name: Paul Mishkin

Title/Position: Chief Executive Officer

### 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:

Date:

BY:

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:**

**Title:**

**Email Address:**

# <u>EXHIBIT “F”</u>

DATA SECURITY REQUIREMENTS

[INSERT DATA SECURITY REQUIREMENTS /FRAMEWORK UTILIZED BY VENDOR HERE AND LOCATION(S) WHERE STUDENT DATA IS STORED]

**Student Data is stored in the United States.**

**See attached “IXL Information Security Policies and Procedures.”**
**See attached “Letter of Engagement - SOC 2 Audit.”**

# EXHIBIT "G"

## DE-IDENTIFICATION OF STUDENT DATA

[COMPLETE THIS FORM IF PROVIDER DESIRES TO DE-IDENTIFY STUDENT DATA PURSUANT TO ARTICLE IV]

1. Check reason(s) for de-identification:

   _assisting the LEA or other governmental agencies in conducting research and other studies

   X research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services;

   X for adaptive learning purposes and for customized student learning

2. Describe de-identification methodology [use separate sheet if needed]:

   [Note: LEA will consider whether methodology includes removal of all direct and indirect identifiers and takes into account the cumulative reidentification risk from previous data releases and other reasonably available information, including publicly-available directory information]

The de-identification process is an internally-defined process in which all user PII fields in our database, for the user(s) being de-identified, are either erased or replaced with fully random values. This process is not reversible.

| IXL.com | |
|---|---|
| Data deletion request | Upon receiving an authenticated request from the account owner, IXL will delete the database records for all or the requested portions of the account, including roster and scoring information. IXL will retain financial information such as payment records. |
| What happens to data backups | Some data may persist in IXL's database backups for 2 weeks after it is deleted. After this time, the older backups are discarded. |
| Upon account expiration/cancellation | After an account on IXL has expired or canceled for 18 months, IXL will automatically de-identify the database data for the account. IXL can accelerate the schedule for deletion or de-identification if requested by the account owner.<br>Notes: Automatic de-identification happens daily using Cron jobs for inactive accounts. |

3. Does Provider plan to transfer De-Identified Student Data to any party (other than Subprocessors)? If so, identify name, purpose and confirm that you will obtain that party's written agreement not to attempt re-identification prior to transferring de- identified data to that party.

No, Provider will not transfer student data to any party.

## Approval of LEA

Authorized Representative of LEA

Printed Name: Kirstin Collins Signature: Date: 9/8/23

Title Director of Technology

## IXL Information Security Policies and Procedures

### Introduction

IXL's information security is a top priority to the company. IXL employs reasonable organizational and technical means to prevent unauthorized access, use, alteration, or disclosure of customer data stored on systems under IXL's control.

1. **Access to customer data.** IXL limits its personnel's access to customer data as follows:
   - Requires unique user credentials and two-factor authentication to access network environments containing user data;
   - External connections to all production systems are limited to encrypted and secure protocols, and governed by firewall rules that grant the minimal amount of access required to perform required functions; and
   - Limits access to customer data to employees with a business need for access.

2. **Data encryption.** IXL provides encryption for customer data as follows:
   - Network connections to IXL's production environment utilize Transport Layer Security (TLS) or Secure Shell (SSH);
   - All data stored in IXL's production environment is encrypted at rest using AES-256 bit encryption; and
   - All data stored on IXL-owned laptops is encrypted at rest.

3. **Data Security Measures**
   - IXL employs automated log collection and audit trails for production systems.
   - Connections originating from untrusted networks segments will be governed by firewall rules and other security safeguards that grant the minimal access required to access the intended service provided by the company.
   - System passwords and access keys are stored in a privileged location accessible only to IXL security administrators, and all credentials are changed from factory default settings.
   - Production systems receive regular maintenance to apply security patches; and
   - Physical access to systems requires security RFID badges and biometric authentication, and is limited to IT staff performing physical maintenance.

4. **Independent security assessments.** IXL utilizes the following third-party services to evaluate and certify IXL's security methodology:
   - Undergoes monthly third-party network vulnerability scanning and assessment tests;
   - Maintains PCI-DSS Compliance Level 2

**5. Incident response.** In the event of a data breach, a thorough post mortem will be conducted to identify the cause and scope of the breach, systems will be patched in a timely manner if necessary, and changes to security methodology will be implemented if warranted. IXL will also comply with any contractual and legal obligations regarding notification of data breaches.

**6. Personnel Management.** IXL requires its employees to conform to information security standards as follows:

- Performs employment verification, including proof of identity validation and criminal background checks for all new hire;
- Conducts on-going training with IXL employees on network security practices and company data handling procedures; and
- Revokes employee access to IXL networks and services upon departure from the company.

**7. Modifications to policy.** From time to time, IXL may modify this policy and its security procedures, but will not materially reduce the overall level of information security. IXL will provide any updates to policy upon request.

Last Modified: February 17, 2022

Date: August 11, 2023

From: IXL Learning, Inc.

Re: Letter of engagement - SOC 2 audit

To whom it may concern:

The purpose of this document is to state IXL Learning, Inc.'s ("IXL") intent to engage in a SOC 2 audit.

IXL is in the process of scheduling a SOC 2 audit, starting with a SOC 2 Type 1 audit, followed by a SOC 2 Type 2 audit in 2024. We will initiate the audit with a focus on the "Security" trust service criteria/trust principles. IXL has engaged in discussions with various auditing firms to conduct the audit. The selected auditing firm will perform a SOC 2 audit in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). The selected auditing firm will prepare a report to be shared with IXL and the affiliated school district.

Sincerely,

Michael Shafir<br>
General Counsel