

WISCONSIN STUDENT DATA PRIVACY AGREEMENT

School District/Local Education Agency:

Verona Area School District

AND

Provider:

Omega Labs Inc dba Boom Learning

Date:

12/18/2023

This Wisconsin Student Data Privacy Agreement (“DPA”) is entered into by and between the Verona Area School District (hereinafter referred to as “LEA”) and Omega Labs Inc. dba Boom Learning (hereinafter referred to as “Provider”) on 12/18/2023. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a contract dated 12/14/2023 (“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; 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 transmitted to Provider from LEA pursuant to the Service Agreement, 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 these 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 may be further outlined in Exhibit “A” hereto: Boom Cards

See Exhibit A

3. **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”.

See 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 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 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 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 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 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 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, and applicable Wisconsin law.

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.** 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 be subject to criminal background checks in compliance with state and local ordinances.
- b. Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA’s designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
- f. Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding seventy-two (72) 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 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 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, the unauthorized access is attributable to Provider's conduct, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Jason Rubo

Title: Director of Technology

Contact Information:
ruboj@verona.k12.wi.us

The designated representative for the Provider for this Agreement is:

Name: Mary Oemig

Title: Chief Executive Officer

Contact Information:
legal@boomlearning.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: Lillith Leonard

Title: Contracts Administrator

Contact Information:
legal@boomlearning.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 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 Wisconsin Student Data Privacy Agreement as of the last day noted below.

Provider:

BY:  _____ Date: December 18, 2023

Printed Name: Mary Oemig Title/Position: Chief Executive Officer

Local Education Agency:

BY:  _____ Date: 12/19/2023

Printed Name: Jason Rubo Title/Position: Director of Technology

EXHIBIT "A"

DESCRIPTION OF SERVICES

Boom Cards teaching resources are cloud-resident and -served instructional-material mini-apps such as digital flash/task cards, quizzes, and interactive lessons.

The *Boom Learning* platform includes three elements: creation tools (provided at no charge to all users), data processing and reporting of student performance data (provide at a fee if more than 5 students), and storage for created Boom Cards mini-apps.

Educators create the instructional material mini-apps for personal use, use with colleagues, and/or for distribution (for a fee or no fee) via the Boom Learning Store or through third-party marketplaces.

Boom Cards may be assigned in ways that do not collect data or in ways that use the Boom Learning Reports feature to process and report student performance data.

EXHIBIT "B"
Schedule of Data

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP addresses of users, use of cookies, etc.	<input checked="" type="checkbox"/>
	Other application technology – meta data—please specify: <i>Platform, browser, build number</i>	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application – <i>Last login</i>	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data – please specify: <i>Formative and summative as assigned by the teacher</i>	<input checked="" type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries): <i>Educator to publishing public author feedback</i>	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data: <i>Only to the extent to which an Educator creates or assigns a Boom Cards resource that collects such information</i>	<input checked="" type="checkbox"/>
Demographics	Date of birth	<input type="checkbox"/>
	Place of birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information – please specify: <i>School location can be inferred from teacher's or student's email domain of school account</i>	<input checked="" type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level – <i>can be inferred if Educator provides the information</i>	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs – <i>possible to infer from Educator assigned content</i>	<input checked="" type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information – please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone number	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names – <i>when provided by the Educators</i>	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information – please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email – <i>Where the Educator uses an authentication method that supplies an email</i>	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School District) ID number – <i>where included in student email address (we do not extract it)</i>	<input checked="" type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords - <i>encrypted</i>	<input checked="" type="checkbox"/>
Student Name	First and/or Last – <i>yes as most Educators provide actual names; pseudonyms are allowed</i>	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program – student types 60 wpm, reading program – student reads below grade level) – <i>yes if the Educator assigns using student performance collection; Educators may avoid by using only Fastplay assignments.</i>	<input checked="" type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires – <i>when an Educator assigns a Boom Cards mini-app that functions as a survey or questionnaire</i>	<input checked="" type="checkbox"/>
Student Work	Student generated content (writing, pictures, etc.) – <i>short written answers; eventually, student created decks</i>	<input checked="" type="checkbox"/>
	Other student work data – please specify: <i>fill in the blank, multiple choice, and other responsive choices</i>	<input checked="" type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data – please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>Required data elements for Educators</p> <ul style="list-style-type: none"> • Email – a unique, valid email address • Username – a globally unique string • Password – any string; encrypted • Teacher Nickname – any string • Teacher name – must be a real name • Full address – if making a purchase • Browser and Operating System • Last login date and time <p>Optional data elements for Educators</p> <p>“Classroom” data items are “optional” – they become required if an Educator uses data processing and reporting of student performance data features</p> <p>Classroom username – a globally unique string</p> <p>Classroom password – any string. This password is not stored encrypted, as it is only an access point.</p> <p>Classroom Nickname – any string e.g., “Kindergarten AM” or “Algebra”</p> <p>“Full address” info is required only for purchasing purposes</p> <p>Required data elements for Students</p> <p>Educators can add/delete/rename student accounts at will.</p> <p>Only Educators can reset forgotten student passwords.</p> <ul style="list-style-type: none"> • Username – globally unique string; can be changed by student and Educator • Password – any string; can be changed by student and Educator; encrypted • Nickname – any string; can be changed by student and Educator; can be locked by Educator; may be pseudonymous or a named identifier • Last login date and time <p>Schools shall supply identifiers that comply with the school's policies. If a school elects to use a third-party authentication service (such as Google or Microsoft Single Sign On), the school agrees that it may provide to Boom Learning the information required to authenticate students. The authenticator may deliver a persistent identifier, name, email address, and an avatar.</p> <p>Collected student progress data elements</p> <p>When students play lessons with progress reporting enabled, Boom Learning collects the following information:</p> <ul style="list-style-type: none"> • Device info: (browser version, OS type) • Time spent • Student responses. 	<input checked="" type="checkbox"/>
None		<input type="checkbox"/>

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: The term “Operator” means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means 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 Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

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

School District Official: For the purposes of this Agreement 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 student 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 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

[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:

<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 By (Insert Date) _____ [Insert or attach special instructions]

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
[INSERT ORIGINATION LEA NAME]

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Name of LEA] 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:

BY:  _____
Mary Oemig (Dec 19, 2023 09:01 PST)

Date: December 18, 2023

Printed Name: Mary Oemig

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:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: Lillith Leonard

Title: Contracts Administrator

Email Address: legal@boomlearning.com

EXHIBIT "F"

Provider's General Privacy Notice is attached and incorporated.

General Privacy Notice

Modified on: Fri, 25 Aug, 2023 at 1:30 PM

EFFECTIVE JULY 1, 2023 ((<https://help.boomlearning.com/en/support/solutions/folders/16000095966>)**see archived version** (<https://help.boomlearning.com/en/support/solutions/articles/16000156247-general-privacy-notice-2021-2022->))





Our Guiding Principles

- Practice makes progress.
- It is okay to make mistakes.
- Mistakes made as a child should not haunt you.
- It is okay to say: “I don’t want everyone to know I’m online.”
- You should know how companies use what they know about you.

1. Who Does This Notice Apply To?

This notice applies to data processed by the Boom Learning web app, iOS app, Android app, and Kindle Fire app (the "Services"). It is part of our Terms of Service. It includes all these supplemental notices. Read them.

1. [KID-FRIENDLY PRIVACY NOTICE](https://help.boomlearning.com/en/support/solutions/articles/16000144383-kid-friendly-student-privacy-notice) (<https://help.boomlearning.com/en/support/solutions/articles/16000144383-kid-friendly-student-privacy-notice>)
2. [INFORMATION SECURITY PLAN](https://help.boomlearning.com/en/support/solutions/articles/16000121794-information-security-plan) (<https://help.boomlearning.com/en/support/solutions/articles/16000121794-information-security-plan>)
3. [DATA ELEMENTS DISCLOSURE](https://help.boomlearning.com/en/support/solutions/articles/16000087842-data-elements) (<https://help.boomlearning.com/en/support/solutions/articles/16000087842-data-elements>)
4. [SUBPROCESSOR DISCLOSURE](https://help.boomlearning.com/en/support/solutions/articles/16000121757-subcontractor-and-subprocessor-disclosure) (<https://help.boomlearning.com/en/support/solutions/articles/16000121757-subcontractor-and-subprocessor-disclosure>)
5. [CONSUMER PRIVACY PROTECTIONS NOTICE](https://help.boomlearning.com/en/support/solutions/articles/16000130809-consumer-privacy-protections-notice) (<https://help.boomlearning.com/en/support/solutions/articles/16000130809-consumer-privacy-protections-notice>)
6. [NON- US DATA SUBJECT PRIVACY NOTICE](https://help.boomlearning.com/en/support/solutions/articles/16000121733-privacy-notice-for-data-exporters-of-data-about-non-us-data-subjects) (<https://help.boomlearning.com/en/support/solutions/articles/16000121733-privacy-notice-for-data-exporters-of-data-about-non-us-data-subjects>)

We made these separate documents to allow you to link to them from your website or to include them in parent notices. You can access our Cookie Notices from our cookie consent dialogue boxes.

You agree that you have the legal right to agree to these notices, which tell you your roles and obligations, for your entity.

Additional privacy information that applies solely to Public Authors is found in the [Public Author Terms of Service](https://help.boomlearning.com/en/support/solutions/articles/16000121727-public-author-terms-of-service) (<https://help.boomlearning.com/en/support/solutions/articles/16000121727-public-author-terms-of-service>).

2. Other Ways to Have Your Privacy Protected

We must have binding privacy agreements in place. We cannot accept any Purchase Order with terms that would effectively ask us to proceed without a privacy agreement.

Government Entities may sign and return our [Government Entity Master Agreement](https://help.boomlearning.com/en/support/solutions/articles/16000121732-government-entity-terms-of-service)

(<https://help.boomlearning.com/en/support/solutions/articles/16000121732-government-entity-terms-of-service>) or our [Government Entity Master Agreement – Canada](https://help.boomlearning.com/en/support/solutions/articles/16000149960-government-entity-terms-of-service-canada)

(<https://help.boomlearning.com/en/support/solutions/articles/16000149960-government-entity-terms-of-service-canada>)

to change our Terms of Service and Privacy Notices. Contact us if you want an alternate agreement. If we have a direct privacy agreement with your district, state, or purchasing entity, those terms will win where they conflict with the terms in this notice.

3. We Are Service Providers

Our business purposes are

- To act as your service provider to enable you, an Educator, to make, share, buy, sell, and assign digital educational resources (Boom Cards) that mostly grade themselves;
- To act as your service provider to enable you, an Educator, to get rapid student performance reports so you have more time to teach and can intervene and accelerate learning.

Collectively we call these the “**Services**”. To provide the Services, we use personal information we receive from you (Adult Data). We also use student personal information, student records, or student-generated content (Student Data) we receive from your students that you have decided to send us. We call all this data User Data.

Educators make accounts for the students they are in charge of. Although minors may use Boom Learning, a responsible adult Educator must accept the terms and set up accounts for the minor. Educators must ensure they have a legal right or actual consent from parents to set up accounts. This will vary from place to place so check with your entity. Parents and legal guardians who are homeschooling or after schooling their children may use the product as Educators.

Some United States schools are governed by the Family Educational Rights and Privacy Act (“**FERPA**”). These schools agree they are engaging us to process Student Data for them. We are doing work for the school for which a school would otherwise use employees. The school tells us what it wants us to do when it comes to use of education

records. We agree that we use and maintain these records for a legitimate educational interest. We use Student Data for the purpose of fulfilling our duties and providing and improving services under this agreement, and nothing else. FERPA entities provide COPPA consent through *in parentis loci*.

“**COPPA**” is the Children’s Online Privacy Act. You may be an entity covered by COPPA but which cannot consent *in parentis loci* because you are not a FERPA entity (for example, you are a private music tutor). If this is you, you must obtain consent from the parent or guardian before creating a student account as part of your normal business service. If you can pay us and we can verify an email address, we assume you are an adult. Educator accounts are for adults only. If we learn that a minor has created an Educator account, we will delete the account and all of the data in it as soon as possible.

You may collect User Data for health therapy interventions. This collection must be consistent with the Health Insurance Portability and Accountability Act (“**HIPAA**”). You must have consent to collect this data. You must also use pseudonyms and private rosters to protect the medical information of patients. You may need to obtain consent under COPPA too.

4. We Do Not Sell Data

We do not sell User Data. See also our notice regarding [Consumer Privacy Protections Notice](https://help.boomlearning.com/en/support/solutions/articles/16000130809-consumer-privacy-protections-notice) (<https://help.boomlearning.com/en/support/solutions/articles/16000130809-consumer-privacy-protections-notice>).

5. How To Contact Us and Changes

Boom Learning is a trade name of Omega Labs Inc. We are a Washington state C Corporation. Our mailing address is 9805 NE 116th St. Suite 7198, Kirkland, WA 98034. You can call us at 833-969-2666. You can contact us to ask questions about this policy or to send us notices.

We will not make material changes to the terms, including our Privacy Notices, without first providing notice via our newsletter service. A material change is one that changes your duties or ours. These things do not count as a material change:

- Reorganizing components between cross-referenced documents.
- Adding detail previously stated in our FAQs if it doesn’t change your duties or ours.

You can review previous versions of the notices in our archive. Any version of this Privacy Notice in a language other than English is provided for convenience. The English language version will control if there is any conflict.

6. User Data we collect and its disclosure

We detail the User Data collected from Students, Educators, and Public Authors in our [Data Elements](https://help.boomlearning.com/en/support/solutions/articles/16000087842-data-elements) (<https://help.boomlearning.com/en/support/solutions/articles/16000087842-data-elements>). We collect some User Data for security monitoring. Most data elements are optional. We give Educators self-help controls that may be used to

retrieve, correct, delete, or restrict User Data. We don't analyze, process, serve, or transfer Student Data until you tell us to by opening an account, adding students, and assigning resources to them. As an Educator, you may update or change most information you have provided to us.

We retain information we must maintain for our business purposes, including but not limited to:

- at least one login authenticator if you are maintaining an active account;
- Boom Cards decks you have sold or shared to other Educators;
- logs for detecting security incidents, deception, and malicious activity;
- logs for detecting fraud and other illegal activity;
- records for internal uses, including debugging and repairing errors, transaction and payment records, and the like; and
- data legally required to be maintained (such as tax-related and financial data).

Student Data is deemed confidential. Educators who enable the classroom roster will display student nicknames to all students on the roster.

Student Data may be disclosed as follows:

- to the student.
- to the Educator who created the student account.
- to the Entity employing that Educator, if any.
- to an Educator provided the information through Educator to Educator student sharing.
- to parents and legal guardians who observe the student dashboard.

7. Data Subject Requests

Parents and students may review Student Data by reviewing the student dashboard with the student or by asking the Educator to show the teacher dashboard for that student. If you are a student or a patient, you must contact the entity who collected the information about you if you are making a data subject request. If you are a parent who wants to review or delete Student Data, contact your Student's Educator. We will not release information to a person other than an Educator unless we are provided satisfactory proof of a legal right to disclose, review, or delete student information.

Everyone else may contact us to learn which personal information we have collected about you. You must make your request in a way that lets us properly understand, evaluate, and respond to it. We will help you delete personal information if you can prove who you are. You will also have to

- provide enough information for us to reasonably prove that you are the owner of the personal information we collected; or
- prove the owner of the personal information said you are allowed to access it;

You may not assign a resource that collects sensitive data unless you have all the required consents. Depending on your governing jurisdiction, these things may be considered sensitive information:

- political affiliation;
- trade union membership;
- health information;
- sexuality information;
- information about protected relationships such as lawyers or ministers;
- criminal behavior;
- firearm ownership;
- and/or biometric data.

You are solely responsible for understanding what you may or may not assign in your jurisdiction.

You agree to indemnify Boom Learning for any liability arising from your actions if you assign a resource that collects information in violation of law. You also agree Boom Learning shall not be liable if you fail to provide a student with the required information regarding their rights. If in doubt, consult your legal counsel and governing body.

8. Subprocessors

Our [subprocessor disclosure](https://help.boomlearning.com/en/support/solutions/articles/16000121757-subprocessor-disclosure) (<https://help.boomlearning.com/en/support/solutions/articles/16000121757-subprocessor-disclosure>) details our sharing of data with our subprocessors. It also discusses your responsibilities with respect to Educator selected subprocessors. Read it carefully.

9. Information Security Plan – Including Security Incidents and Deletion

Our [Information Security Plan](https://help.boomlearning.com/en/support/solutions/articles/16000121794-information-security-plan) (<https://help.boomlearning.com/en/support/solutions/articles/16000121794-information-security-plan>) includes our policies on security incidents, backups, deletion, encryption, and more.

You agree to use Boom Learning in a way that protects you and your students' data. This includes providing or getting adequate training on the use of secure authentication and the dangers of open networks. It also includes obtaining secure networks on which to use Boom Learning. You agree to use passwords for Educator accounts that are adequately secure to prevent intrusion. It is up to you to keep your login information confidential.

You will take reasonable steps to ensure that any of your employees, agents, or independent contractors who have access to Student Data are reliable. This includes volunteers.

Reasonable steps include:

- making sure access is limited to those with a need to know and access the Student Data;
- conducting background checks if required;
- making sure that all these people are required to keep data confidential; and
- training these people on security and privacy requirements for your organization.

You agree that we are not liable for any regulatory penalties or other liabilities that arise when you fail to comply with your data security responsibilities. Boom Learning will only be liable for its own failures and those of its selected subprocessors.

10. No Advertising to Students; Adults Opt In

We direct our marketing to Educators; never to students.

Educators are either Direct Purchase Educators or Managed Teachers. Managed Teachers are associated with a buying entity such as a school or clinic. Managed Teachers can only opt in to email promotional offers if their entity contract permits them to opt in. Administrators of Managed Teacher accounts may contact our **sales team** to ask about discounts or special offers available to entities.

Direct Purchase Educators may be presented with discount and reward offers for Boom Cards or Boom subscriptions from time to time. Offers are primarily communicated through our landing pages, our blog, estimator tool, and social media. We also allow Direct Purchase Educators to **opt in** to receive email offers or special offers from select sellers. These offers are covered by our separate Privacy Policy for advertising and marketing **here** (<https://blog.boomlearning.com/privacy-policy/>).

We provide All Educators with recommendations based on the Educator choices made for the populations they serve to further our shared goal of providing education. You agree that Boom Learning is permitted to inform Educators of training opportunities, new Boom Cards, or Boom Learning features or functionality.

11. Legal authority data requests

We are required to disclose User Data in response to lawful requests. This includes requests by national security and law enforcement officials. In the event a legal authority asks to access your data, we will direct the requestor to you. We will await your consent, unless we are legally compelled to act without getting your consent. If we are legally compelled to act, we will promptly notify you and provide you with a copy of the request unless legally prohibited from doing so. If a legal authority is asking for information about a student, you agree to pass the notification to the student's legal guardian and you indemnify us for your failure to do so.






wi_Verona Area SD_NDPA 2023 - modified

Final Audit Report

2023-12-19

Created:	2023-12-18
By:	Lillith Leonard (lillith@boomlearning.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAguQcUo5iw_8kCDEHy54a0Mh-R_vVUEe

"wi_Verona Area SD_NDPA 2023 - modified" History

-  Document created by Lillith Leonard (lillith@boomlearning.com)
2023-12-18 - 7:13:22 PM GMT- IP address: 24.18.32.67
-  Document emailed to Mary Oemig (mary@boomlearning.com) for signature
2023-12-18 - 7:14:51 PM GMT
-  Email viewed by Mary Oemig (mary@boomlearning.com)
2023-12-19 - 4:59:42 PM GMT- IP address: 104.47.56.254
-  Document e-signed by Mary Oemig (mary@boomlearning.com)
Signature Date: 2023-12-19 - 5:01:07 PM GMT - Time Source: server- IP address: 50.47.87.221
-  Agreement completed.
2023-12-19 - 5:01:07 PM GMT