

STANDARD STUDENT DATA PRIVACY AGREEMENT

WA-NDPA Standard

Version 1.0

Local Education Agency (LEA):

Evergreen School District #114

and

Provider:

Pioneer Valley Educational Press, Inc. dba Pioneer Valley Books

DATE:

11/8/24

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

School District: Evergreen School District #114 , located at: 13413 NE LeRoy Haagen Dr Vancouver WA (“**LEA**”) and
Provider: Pioneer Valley Educational Press, Inc dba Pioneer Valley Books , located at: 199 Pine Street, Florence, MA 01062 (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required.**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms of modifications set forth in **Exhibit “H”**
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. [Reserved]
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Alison Garcia Title: Senior Business Development Specialist

Address: 199 Pine Street, Florence, MA 01062

Phone: 888.482.3906 Email: privacy@pioneervalleybooks.com

The designated representative for the LEA for this DPA is:

Name: _____ Title: _____

Address: 13413 NE LeRoy Haagen Dr Vancouver WA

Phone: _____ Email: _____

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Evergreen School District #114

By:  Date: 11/13/2024

Printed Name: Dr. Christine Moloney Title/Position: Superintendent

Name of Provider: Pioneer Valley Educational Press, Inc. dba Pioneer Valley Books

By: *Alison Garcia* Date: 11/8/24

Printed Name: Alison Garcia Title/Position: Senior Business Development Specialist

STANDARD CLAUSES

Version 3.0

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 federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **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 any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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 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 Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct, as necessary. In the event that a parent of a student 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 Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
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 outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. [See Modification at Exhibit "G"]
3. **Provider Employee Obligation**. Provider shall require all of Provider's 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. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on

behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (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 purpose and for customized student learning. 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 from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. [See modification at Exhibit "G"]

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. 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 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.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements 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.
 - (3) 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 summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) 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 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 **Exhibit "E"** 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. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.

5. **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.

6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. 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.

8. **Authority.** Each party 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.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Pioneer Valley Books will provide access to the Literacy Footprints Digital Reader. Service includes a library of digital books, student access in school or remotely, teacher tools for progress monitoring, and teacher assignment tools. Access is granted for the 2024-2025 academic year.

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 type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input 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)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input 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:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input 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	<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"/>
Schedule	Student scheduled courses	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Teacher names	<input 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	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input 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	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input 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"/>
	Students 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	Please list each additional data element used, stored, or collected by your application:	<input data-bbox="1344 688 1393 741" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input data-bbox="1344 1283 1393 1335" type="checkbox"/>

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information 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 educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials 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.

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 Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “student-generated content” means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

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 service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

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 Education Records and/or Student Data, as that term is used in some state statutes. 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

District or LEA: Evergreen School District #114 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:

1. Extent of Disposition

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Categories of data:

Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Special instructions:

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By Date:

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Evergreen School District #114 ("Originating LEA") which is dated 11/8/24, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through 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 Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material changes in the applicable privacy statutes; (2) a material changes in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Name of Provider: Pioneer Valley Educational Press, Inc. dba Pioneer Valley Books

BY: *Alison Garcia* Date: 11/8/24

Printed Name: Alison Garcia Title/Position: Senior Business Development Specialist

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 for the term of the DPA between originating LEA: Evergreen School District #114 and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

Name of Subscribing LEA:

By: *Christine Moloney* Date: 11/13/2024

Printed Name: Dr. Christine Moloney Title/Position: Superintendent

SCHOOL DISTRICT NAME: Evergreen Public Schools

DESIGNATED REPRESENTATIVE OF LEA:

Name: W. Bryce Rea

Title: Manager, IT Systems & Security

Address: 13413 NE LeRoy Haagen Memorial Drive, Vancouver, WA 98684

Telephone Number: 360-604-4096

Email: william.rea@evergreenps.org

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

<input type="checkbox"/>	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

EXHIBIT "G" – Supplemental SDPC State Terms for [State]

Version 1.0

1. Recitals shall have the following sections added: This Amendment for SDPC State Terms for Washington ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

School District: Evergreen School District #114, located at: 13413 NE LeRoy Haagen Dr Vancouver WA (the "**LEA**") and
Provider Name: Pioneer Valley Educational Press, Inc. (the Pioneer V.), located at: 199 Pine Street, Florence, MA 01062 (the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws;

WHEREAS, the Provider will provide the services to LEA within the State of Washington and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable Washington laws and regulations, such as the Student User Privacy in Education Rights 28.A.604 et seq. and RCW 42.56.590; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable Washington state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. **Term**. The term of this Amendment shall expire on the same date as the DPA.
2. **Modification to Article IV, Section 2 of the DPA**. Article 4, Section 2 of the DPA is hereby amended to read as follows:

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 outlined in Exhibit "A" or stated in the Service Agreement, or authorized under the statutes referred to herein by this DPA. Provider may use or disclose data to:

- (a) Protect the security or integrity of its website, mobile application or online service.
- (b) Ensure legal or regulatory compliance or to take precautions against liability.
- (c) Respond to or participate in the judicial process.
- (d) Protect the safety of users or others on the website, mobile application or online service.
- (e) Investigate a matter related to public safety.

In undertaking the activities specified in subsections (a) through (e) above, Provider shall adhere to all applicable data protections contained in this DPA, as well as Federal and Washington State law.

3. **Modification to Article IV, Section 7 of the DPA**, Article IV, section 7 is hereby amended to add the following language:

(iv) providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part or other consideration from a third party.

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Evergreen School District #114

By:  Date: 11/13/2024
 Printed Name: Dr. Christine Moloney Title/Position: Superintendent

Provider: Pioneer Valley Educational Press, Inc. dba Pioneer Valley Books


By:  Date: 11/8/24
 Printed Name: Alison Garcia Title/Position: Senior Business Development Specialist

EXHIBIT "H" – Additional Terms or Modifications

Version 1.0

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

830-1/6107877.1

Expiration Date: 08/31/2025

Pioneer Valley Educational Press, Inc. Privacy Policy for Digital Reader

Last Modified: July 15, 2024

Pioneer Valley Educational Press, Inc. (“PVEP”) is committed to protecting your privacy. In this Privacy Policy (“Policy”), we describe how we collect, use, and disclose information that we obtain about visitors to www.digitalreader.com (the “Site”) and users of the digital reader service available through our Site (the “Service”).

Consent

By visiting the Site or using our Service, you agree that your information will be handled as described in this Policy. Your use of our Site or Service, is subject to this Policy, including its applicable limitations on damages and resolution of disputes.

A Note about Student Data

Our Service may be used by a school, school district, or teacher (collectively referred to as a “School”) in a classroom or remote learning setting. Through the provision of our Service to a School, we may collect personally identifiable information from or about students (“Student Data”). We consider Student Data to be highly confidential and do not use such data for any purpose other than providing our Service to the School and as otherwise provided in our agreements with the School. If you have any questions about reviewing, modifying, or deleting personal information of a student, please contact your School directly.

What Information Do We Collect?

We collect information both directly from you and automatically when you visit our Site or use the Service.

Information We Collect Directly

- **School and Teacher Information.** When a School registers for an account on our Service or corresponds with us online, we collect certain personal information to use such as a name, email address, username, and password. We may also collect additional information about the School, such as a school or district identifier, information about teachers and others authorized to use the Service.
- **Student Information.** Once registered, a School may provide information about its students, such as a name or other identifier, email, year of study, and current estimated reading level. The School may elect to provide non-personally identifiable usernames or identifiers in lieu of a full student name, at its discretion.
- **Parent Information.** We may collect information about a student’s parent or guardian, such as name and email address, if provided by the School.

Information We Collect Automatically

Like most websites and online services, we automatically collect certain types of information about visitors to our Site and users of our Service through cookies and other similar technologies. Examples include referring URL; browser type and version; device name and model; operating system type, name, and version; web pages viewed; links clicked; and length of time spent engaged with the Site and the Service. We do not collect or store your IP address. Although we do our best to honor the privacy preferences of our visitors, we are not able to respond to Do Not Track signals from your browser at this time.

We use this automatically collected information to (i) improve user experience and personalize your content; (ii) provide and monitor the effectiveness of our Service; (iii) monitor aggregate metrics, such as total number of visitors, traffic, usage, and demographic patterns on our Site and our Service; (iv) diagnose or fix technology problems; (v) investigate fraud or misuse of the Service; and (vi) otherwise plan for and enhance our Service.

Cookies are required to support most features of the Site. We use cookies to enable authenticated user sessions, which are required for all areas of the Site that deliver personalized content to the user such as our book reader. The information we store using cookies is not, in and of itself, personally identifiable, but we may link it to personal information that users have provided. If you do not wish to receive cookies, you may set your browser to reject cookies or to alert you when a cookie is placed on your computer. Although you are not required to accept cookies when you visit this Site, you may be unable to use all of the functionality of this Site if your browser rejects our cookies.

How Do We Use Your Information?

We collect information for the following purposes:

- **Provision of Services:** To provide our Service, to communicate with School users, to respond to inquiries, and for other customer service purposes.
- **Reporting:** To provide students and teachers with information and reports about student performance and use of the Service.
- **Personalization:** To tailor the content and information that we may send or display to users, to offer personalized help and instructions, and to otherwise personalize your experience while using the Service.
- **Transactional Notifications:** To provide notifications for certain activities relating to your use of our Service. For example, we send you notices when your assessments have been scored.
- **Marketing Communications:** From time to time, to send periodic promotional or informational emails to School users. We do not use Student Data to send marketing communications. You may opt out of such communications by following the opt-out instructions contained in each email.
- **Statistics:** To collect statistics to better understand how users access and use our Site and Service in order to improve our Site and Service and for other research and analytic purposes.

- **Product Improvement and Development:** To maintain, develop, support, and improve our Service and our other educational products and services.

How Do We Share Your Information?

We do not sell or share your personal information with third parties for marketing purposes. We may share your personal information in the following ways:

- **Other School Users.** Depending on your account settings and permissions, we permit information to be shared between and among authorized School users. For example, teachers, schools, and school districts can see information about their students' activities on the Service. Information associated with a school or school district is restricted to users within that same school or school district only and not shared with any other schools or school districts using the Service.
- **Consent.** We may share information with consent and at the direction of a School or parent. For example, if a School user directs us to, we will share content with the parent or guardian of a student.
- **Service Providers.** We may disclose personal information with our trusted third-party vendors, service providers, contractors, or agents who perform functions on our behalf, such as payment processing, transcription services, and web hosting. Personal information will be shared with these third parties as needed to perform their services to us, under reasonable confidentiality terms.
- **Business Transfers.** We may disclose personal information in the context of a company transaction, such as a merger, sale of company assets or shares, financing, change of control, bankruptcy, or other corporate event. If the transaction involves the transfer of Student Data to a third party, we will require the new owner to continue to honor the terms provided in this Privacy Policy, or we will provide you with notice and an opportunity to opt out of the transfer of Student Data by terminating your account and deleting your data before the transfer occurs.
- **In Response to Legal Process.** We may disclose information as required or authorized by law, a judicial proceeding, court order, or other legal process. When legally permitted, we shall strive to notify the School of any legal request to access Student Data before we respond to such request.
- **To Protect PVEP and Others.** We also may disclose information where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of this Policy, or as evidence in litigation in which PVEP is involved.
- **Aggregate and De-Identified Information.** We may share aggregate or de-identified information that does not reasonably identify you as an individual with third parties for research, marketing, advertising, or similar purposes.
- **Security of Personal Information** The security of your personal information is important to us. We have implemented a variety of physical, administrative, and technological safeguards designed to preserve the integrity and security of all personal information we collect. Our employees and contractors are required to protect personal information in a manner consistent with the terms of this Privacy Policy, and violators will

be subject to disciplinary action, up to and including termination and further legal action. Please be aware that despite our best efforts, no data security measures are impenetrable, and we cannot guarantee the security of our systems 100%. In the event that any personal information under our control is compromised as a result of a breach of security, we will take reasonable steps to investigate the situation and take all steps required by law and current regulations. You should take steps to protect against unauthorized access to your password, phone, and computer by, among other things, signing off after using a shared device, choosing a unique and robust password, and keeping your login and password private. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account resulting from a third party's unauthorized use of or access to your password and account.

Reviewing and Modifying Information

Upon request, we will provide Schools with an opportunity to review, modify, and/or delete the personal information collected from their students. If you are a parent and have questions about your child's use of our Service and any information collected, you should discuss your questions with your child's School, which will submit the request to PVEP at the School's discretion.

Retention and Deletion

We will retain your information for as long as necessary for the identified purpose, which may extend beyond the termination of our relationship with you. For example, we may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, or if required by law. We may retain indefinitely information that has been de-identified or aggregated such that it can no longer reasonably identify a particular individual. All retained personal information will remain subject to the terms of this Privacy Policy. Otherwise, we will delete personal information upon request or according to our standard data retention schedule.

We will not knowingly retain Student Data beyond the time period required to support an educational purpose, unless authorized by the School or parent, and will delete Student Data promptly upon request from the School. Under our current data retention schedule, we will delete Student Data and other information provided to us by a School for academic terms that have ended over two years ago. To the extent the School wishes to retain such Student Data or other School-provided information, the School is responsible for exporting all such records within two years of completing an academic term and/or for storing and maintaining such Student Data and School-provided information independent of the Site or the Service.

Under our current data retention schedule, we retain Student Data for a period of six months after termination of the contract to continue to provide the School access to its records and aggregate reports, after which the Student Data will be deleted and/or de-identified, unless we receive a deletion request from a School prior to that date. We will not be required to delete any information that has been de-identified or disassociated with personal identifiers such that it can no longer be used to reasonably identify a particular individual.

Compliance with Laws

Our collection, use, and disclosure of Student Data is governed by any other agreement with the School, by the provisions of the Family Educational Rights and Privacy Act (“FERPA”), the Children’s Online Privacy Protection Act (“COPPA”), and applicable state laws relating to the collection and use of personal information of students. If you have any questions about our collection and use of Student Data, please contact us at privacy@pioneervalleybooks.com. If you have any questions about reviewing, modifying, or deleting the personal information of a student, please contact your School directly.

The Family Educational Rights and Privacy Act (“FERPA”)

This Privacy Policy and our Service are designed to meet our responsibilities to protect personal information from the students’ educational records under FERPA. We agree to work with each School to jointly ensure compliance with FERPA regulations.

The Children’s Online Privacy Protection Act (“COPPA”)

This Privacy Policy and our Service are designed to comply with COPPA. We do not knowingly collect personal information from a child under 13 unless and until a School has authorized us to collect such information through the provision of the Service on the School’s behalf. When a School uses our Service in the classroom or in an educational context, we rely on the School to provide appropriate consent and authorization for a student under 13 to use the Service and for PVEP to collect personal information from such student, as permitted by COPPA. Upon request, we will provide school users with an opportunity to review and delete the personal information collected from their students. If you are a parent and you have questions about your child’s use of our Service and any information collected, you should discuss your questions with your child’s School.

Students Online Personal Information Protection Act (“SOPIPA”)

This Privacy Policy and our Service are designed to comply with SOPIPA. We do not engage in targeted advertising based on information that we collect through our Service. We do not use collected information to amass student profiles except in furtherance School purposes. We never sell Student Data unless the sale is part of a corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets, in which case we will use our best efforts to ensure the successor entity honors the privacy commitments made in this policy and/or we will notify you of such a sale and provide you an opportunity to opt out by deleting your account before the data transfer occurs.

Forum Selection

In the event that there is a dispute concerning this Privacy Policy or its subject matter, such dispute shall be litigated in the courts of the Commonwealth of Massachusetts in Hampshire County, Massachusetts, or in the Western Division of the United States District Court for District of Massachusetts.

Limitations on Liability

In no event will PVEP be liable for any special, incidental, indirect, or consequential damages whatsoever arising from your access or use of, or inability to access or use, the Site or the Service.

In no event with PVEP be liable for any damages whatsoever arising in any way from any act or omission by any other person including, without limitation, any content provided, or representation made, by another person.

In any event, PVEP's entire liability to you under any provision of this Privacy Policy or arising from the access or use of the Site or the Service by you or any other user will be limited to the amount actually paid by you to PVEP for use of the Site or the Service during the 12 months preceding the event giving rise to such liability.

Changes to This Policy

This Policy is current as of the Effective Date set forth below. If we make any material changes to this Policy, we will post those changes here. We encourage you to periodically review this page for the latest information on our privacy practices. Your continued use of the Site and Service signifies your acceptance of any changes.

We will not make any material changes to our Privacy Policy that relate to the collection or use of Student Data without first giving notice to the School and providing a choice before Student Data is used in a materially different manner than was disclosed when the information was collected.

Contact Us

If you have questions about the privacy aspects of our Service, please contact us at privacy@pioneervalleybooks.com.

Effective Date

PVEP's Privacy Policy has been published and in effect since at least as early as April 7, 2020. This version, which is specific to the Digital Reader, was last updated July 15, 2024

SCHEDULE OF DATA – EXHIBIT “B”

Category of Data	Elements	Check If Used By Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data <ul style="list-style-type: none"> • Please specify: Browser type and version, OS type 	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	X
	Other assessment data Please specify: Student reading level data, running record data	X
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	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	X
	Year of graduation	
	Other enrollment information- Please specify: Teachers/school admins may provide homeroom information, intervention data	X
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	

Category of Data	Elements	Check If Used By Your System
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	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)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data. Please specify: Data on books read and favorited	X
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	<p>Please list each additional data element used, stored, or collected by your application:</p> <ul style="list-style-type: none"> • Data on student's teacher, group, school, and district • Data on student's reading assignments status (complete/incomplete) • Data on word study and vocabulary performance, option that will allow for teachers to record student reading sessions and responses to questions or activities 	X

**NIST CYBERSECURITY FRAMEWORK:
PIONEER VALLEY BOOKS (PVB) RESPONSE for the
DIGITAL READER APPLICATION**

1. Identify (ID)

1. Asset Management (ID.AM)

1. The infrastructure housing the application will reside outside the company's digital infrastructure. All server and database management services provided to customers by the Digital Reader application will be provided by highly reputable companies operating in the United States. The benefits include enhanced security, more consistent delivery of services and greater reliability of backup and recovery capabilities.

2. Business Environment (ID.BE)

1. Our company's role is focused on the design and development of the application's services needed to meet the educational needs of our customers. This component is headed up by two company owners: President and CEO, Michele Dufresne, and CTO, Nicholas Dufresne. Infrastructure for delivery of services is covered in **1.a**. We have partnered with external legal and technology teams to provide consulting roles on such matters as federal, state and local laws, security, forensics in case of a breach, and system assessment to help improve company cybersecurity processes.

3. Governance (ID.GV)

1. Access to the application and application data is restricted to specific roles used only by the development and support teams.

4. Risk Assessment (ID.RA):

1. Per our strategy (1.e), the assessment and management of risk is largely transferred to external companies. In this way internal cybersecurity risk is limited to a small number of employees and devices that access the application and data.

5. Risk Management Strategy (ID.RM):

1. The company's primary strategy for minimizing security risk is to take advantage of top tier external companies to manage cyber assets and cyber security. This approach minimizes access to customer data by our

company and company employees. Our internal team is being built to take advantage of these external resources and the security options they provide. Internal risk is managed by minimizing access to the application and database by employees.

6. **Supply Chain Risk Management (ID.SC):**
 1. NA
2. **Protect (PR)**
 1. **Identity Management, Authentication and Access Control (PR.AC)**
 1. Access to application and database is accessible to CTO and principal developers on CTO designated devices, with access requiring authentication and encryption keys.
 2. **Awareness and Training (PR.AT)**
 1. CTO, and employees who interact with school districts, are trained to delete/destroy any data (digital or physical) they may come in contact with as part of supporting, or providing service to, customers.
 3. **Data Security (PR.DS):**
 1. Information and records are stored off-site and generally not accessible by employees.
 4. **Information Protection Processes and Procedures (PR.IP)**
 1. NA
 5. **Maintenance (PR.MA)**
 1. Provided by server and database management companies.
 6. **Protective Technology (PR.PT)**
 1. Provided by server and database management companies.
3. **Detect (DE)**
 1. **Anomalies and Events (DE.AE)**
 1. Provided by server and database management companies.
 2. **Security Continuous Monitoring (DE.CM)**
 1. Provided by server and database management companies.
 3. **Detection processes (DE.DP)**

1. Provided by server and database management companies.

4. Respond (RS)

1. Response Planning (RS.RP)

1. Response Plan: (1) CTO will resecure our application and data. (2) Contact our technical partners to support an analysis of the incident and to consult on a response plan.

2. Communications

1. (3) Contact our legal team to support our response to schools consistent with national, state and local laws and with existing contractual agreements. Our legal team will work with a forensic service to support an independent analysis of any security incident.

3. Analysis (RS.AN)

1. As described in parts 4.a and 4.b.

4. Mitigation (RS.MI)

1. As described in parts 4.a and 4.b.

5. Improvements (RS.IM)

1. As described in parts 4.a and 4.b.

5. Recovery (RC)

1. Recovery Planning (RC.RP)

1. We have run a replicated DB server (so we have a backup immediately available), and we also do 6 months of daily snapshots of the database that can be restored if the whole datacenter goes down.

2. Improvements (RC.IM)

1. Per 4.a and 4.b we will use the analyses of our technical partners and independent forensic service to identify weakness in our cybersecurity systems. Working with our technical partners we will research and design improvements to overcome identified weaknesses.

3. Communication (RC.CO)

1. As appropriate.