PIONEER VALLEY BOOKS DATA SECURITY AND PRIVACY PLAN

The Contractor (Pioneer Valley Books) represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

Data collected/used for educational purposes only

Pioneer Valley Books shall use the Data solely for the purpose of providing services as set forth in the parties' Agreement. Pioneer Valley Books and its subcontractors shall use the Data only for educational purposes in order to provide the requested services. Pioneer Valley Books and its subcontractors will not use the Data for any other purposes. Any Data received by Pioneer Valley Books or any of its employees, subcontractors, or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

Administrative, operational and technical safeguards

It is the intent that employees of Pioneer Valley Books will not access Data, except at the request of the school district. Only the Chief Technology Officer (CTO), or a designee of the CTO (but then, only for a limited time and only for the purpose requested by the school district) will have the ability to access data to meet any school district request.

In the event that Pioneer Valley Books subcontracts with an outside entity or individual in order to fulfill its obligations to the District, it will ensure that it will only share the Data with such subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain data privacy and security as required by Pioneer Valley Books pursuant to this Agreement. Pioneer Valley Books will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the Data in its custody.

- We limit access to data. No employee accesses data unless requested to do so by the school/school district.
- Only the Chief Technology Officer/Owner has ability to access data, unless he designates an employee or subcontractor for limited access to support meeting a request of the school district.
- Keys are not stored on work computers and are only accessible by two team members (an alternate to the CTO in case of emergency) requiring 2FA to gain access to the keys.
- We use proven cloud hosting resources: AWS and Heroku. Data is stored in the US.
- We have an experienced external legal team to support response to new legal requirements, school district contract modifications, or a suspected security breach (including notification, forensic analysis, and technical support)

Training provided for employees/subcontractors

By limiting access to the application and school district data to a high-level officer/owner of the company (or a designee in very limited capacity to meet a request of the school district) the complexity of the administrative, operational and technical concerns are minimized. The CTO (and any designee) is required to undergo education concerning security and privacy laws and to sign an NDA.

Data Security and Privacy Incidents/Breaches

We have an experienced external legal team to support response to new legal requirements, school district contract modifications, or a suspected security breach (including notification, forensic analysis, and technical support).

In the event of a breach, suspected or confirmed, of data security, that is reported directly to PVEP's Information Security Coordinator ("ISP"), the ISP will take the following steps:

1. Contact PVEP's CTO, or, if the system is monitored by a vendor, that vendor, immediately, in order to contain and preserve evidence of the breach.

2. Complete or arrange for another knowledgeable party to complete the Initial Incident Response Form appended hereto.

3. Contact legal for determination of whether suspected breach is reportable breach of data security, to establish privilege for future communications and potential forensic investigation of data breach incident.

4. If applicable, contact insurer

5. Within a reasonable time after the incident is resolved, an Incident being "resolved" when notification has been made to at least one consumer or regulator and/or it has been determined that the incident is not a reportable breach under law, complete or arrange for the completion by some knowledgeable person of the Incident Post Mortem Worksheet appended hereto.

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 robust password that nobody else knows or can easily guess, 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 via unauthorized password activity.

Transition or Destruction of Data

The data will be returned to the district upon request. Otherwise the data will be deleted within two years from the end of the service. If we delete or move databases our host can manage a secure wipe. For school data removal no additional security measures are taken beyond deleting the data.

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. We do not delete or de-identify any Student Records associated with an active School contract except at the direction of the School. The School is responsible for maintaining current class rosters and managing Student Data that the School no longer needs for an educational purpose through the School dashboard or by submitting a deletion request.

We retain Student Data for a period of two years 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.

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.	✓
	Other application technology meta data-Please specify: Browser type and version, OS type	✓
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	✓
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	✓
	Homeroom	✓
	Guidance counselor	
	Specific curriculum programs	✓
	Year of graduation	
	Other enrollment information-Please specify: Teachers/school admins may provide homeroom information, intervention data	✓
Parent/Guardian Contact Information	Address	
	Email	

Category of Data	Elements	Check if Used by Your System
	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	✓
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	✓
	Phone	
Student Identifiers	Local (School district) ID number	✓
	State ID number	
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
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	✓
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: 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.	✓
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

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

1. **Identify (ID)**
    a. **Asset Management (ID.AM)**
        i. The infrastructure housing the application will reside outside the company's digital infrastructure. All server and database management services provided to customers by the Literacy Footprints 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.

    b. **Business Environment (ID.BE)**
        i. 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.

    c. **Governance (ID.GV)**
        i. Access to the application and application data is restricted to the CTO, who is an owner of the company. The CTO does not access application data, except as required by an appropriate authority (customer, school district officer, or governmental authority). No external partners have access to data. No employee other than the CTO has access to the database.

    d. **Risk Assessment (ID.RA):**
        i. 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.

    e. Risk Management Strategy (ID.RM):

i. 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.

f. **Supply Chain Risk Management (ID.SC)**:
   i. NA

2. **Protect (PR)**
   a. Identity Management, Authentication and Access Control (PR.AC)
      i. Access to application and database is limited to CTO on CTO designated devices, with access requiring authentication and encryption keys.

   b. Awareness and Training (PR.AT)
      i. 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.

   c. Data Security (PR.DS):
      i. Information and records are stored off-site and generally not accessible by employees.

   d. Information Protection Processes and Procedures (PR.IP)
      i. NA

   e. **Maintenance (PR.MA)**
      i. Provided by server and database management companies.

   f. **Protective Technology (PR.PT)**
      i. Provided by server and database management companies.

3. Detect (DE)
   a. **Anomalies and Events (DE.AE)**
      i. Provided by server and database management companies.

   b. Security Continuous Monitoring (DE.CM)
      i. Provided by server and database management companies.

c. **Detection processes (DE.DP)**
    i. Provided by server and database management companies.

4. **Respond (RS)**
    a. **Response Planning (RS.RP)**
        i. 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.

    b. **Communications**
        i. (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.

    c. **Analysis (RS.AN)**
        i. As described in parts 4.a and 4.b.

    d. **Mitigation (RS.MI)**
        i. As described in parts 4.a and 4.b.

    e. **Improvements (RS.IM)**
        i. As described in parts 4.a and 4.b.

5. **Recovery (RC)**
    a. **Recovery Planning (RC.RP)**
        i. We have run a replicated DB server (so we have a backup immediately available), and we also do 7 day running snapshots of the database that can be restored if the whole datacenter goes down.

    b. **Improvements (RC.IM)**
        i. 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.

    c. **Communication (RC.CO)**
        i. As appropriate.