Data Security and Privacy Plan (DSPP)

Piano Marvel LLC

July 2022

I. Objective and Scope

In providing Software as a Service, Piano Marvel acknowledges that we have a serious obligation to help our clients protect the confidentiality of student and staff data in our custody. As a technology contractor for your Organization (school, school district, university, or educational organization), we recognize that we share certain responsibilities to protect the security and privacy of sensitive data that is collected by the Organization and processed by our systems. This Data Security and Privacy Plan (DSPP) outlines the administrative, technical and physical safeguards used to meet these responsibilities.

Educational data housed in Piano Marvel systems is protected by the Family Education Rights and Privacy Act (FERPA). Personally identifiable information (PII) of students is protected under FERPA, PPRA, COPPA and other federal, state and local regulations, including NY State Education Law section 2-d and California's SOPIPA. Piano Marvel's Privacy Policy strictly prohibits the sale of sensitive student and staff data under any circumstances, or the unauthorized sharing of that data with other parties. Data collected is only used for the approved purposes specified in agreements between Piano Marvel and the client.

II. Data Security and Privacy Obligations

A. Relationship Between Security and Privacy

Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' policies.

B. Shared Responsibility

Privacy regulations define several distinct roles with respect to data:

Data subject/owner	the individual who is described or identified	student, staff
Data controller	organization collecting the data for some defined purpose	client organization
Data processor	provider of technology/services in support of the defined purpose	Piano Marvel

Note that data privacy protection requires cooperation between the data controller (Organization) and the data processor (Piano Marvel). In most cases, there is no direct relationship between Piano Marvel and the data subject/owner. The Organization, as data controller, has the primary responsibility for ensuring that data is protected appropriately throughout all phases of its life cycle.

The Organization's role is to:

- Define their business needs or purpose for collecting data
- Designate personnel responsible for data privacy matters
- Establish privacy policies and practices aligned with the defined purpose
- Communicate directly with students/staff/parents regarding data collection and use
- Obtain consent for data collection as appropriate
- Provide awareness training to ensure that their staff, administrators, and volunteers know how to handle sensitive data properly

Piano Marvel's role is to:

- Communicate privacy objectives to internal users and clients
- Provide the technical means to process data securely
- Protect data while it is in our custody
- Provide awareness training to ensure that our employees know how to handle sensitive data properly

Note that in most cases Piano Marvel does not interact directly with the data subjects; therefore it is the responsibility of the Organization to obtain explicit consent where appropriate. Under the FERPA “school official exception”, explicit consent is not needed when data is collected for the purpose of providing the agreed-upon services, since Piano Marvel is acting as an agent of the Organization.

C. Defining the Purpose

Piano Marvel limits the “purpose” of its systems to the provision of the following broadly-defined services in support of music education within the Organization:

- Uploading and storing Student, Staff, and Organization data voluntarily provided to Piano Marvel.
- Generating data from interactions performed within Piano Marvel.
- Displaying relevant data to authorized individuals.
- Facilitating music learning within the Organization using the provided or generated data.
- Creating reports and summaries of data relevant to the Student, Staff, and Organization.

D. Allowed and Prohibited Access/Use/Disclosure

Student and staff data, whether provided to Piano Marvel by the Organization or generated by Piano Marvel through normal system operation, is only to be used for the above defined purposes. Within Piano Marvel, data is only to be shared with employees who have a legitimate need to access it in connection with the agreed-upon services.

Piano Marvel will not disclose any personally identifiable information to any other party without prior written consent of the Organization, unless required by statute or court order. In this case, we will provide a notice of such disclosure to the Organization no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

E. State/Local Data Privacy Regulations

In accordance with NY State Education Law section 2-d, each district must publish a Parents' Bill of Rights (PBOR), which outlines the Organization's specific student data privacy responsibilities and expectations. Piano Marvel is also in compliance with federal and California privacy law requirements, including FERPA, COPPA, PPRA, and the Student Online Personal Information Protection Act (SOPIPA). Piano Marvel stays continuously updated on evolving privacy regulations. This section outlines the Organization's specific student data privacy responsibilities (as a data controller) and defines Piano Marvel's role (as a data processor) in meeting each of them.

F. Standard Student Data Privacy Practices

1. Restrictions on Use and Release of Student Information

Student and staff data, whether provided to Piano Marvel by the Organization or generated by Piano Marvel through normal system operation, is only to be used for the purposes defined in Section II-C.

In accordance with applicable data privacy laws and Piano Marvel's privacy policy, Piano Marvel will not sell a student's personally identifiable information or release it for any commercial purposes.

Within Piano Marvel, access to student and staff data is only granted to individuals who need such access to perform their job functions. Piano Marvel employees are prohibited from accessing this data for any other purpose. In order to provide the agreed-upon services, it may be necessary to share student or staff information with subcontractors. Piano Marvel ensures that such subcontractors abide by applicable data protection and security requirements.

2. Right to Review

Piano Marvel acknowledges that eligible students or parents (if the student is not eligible as defined by FERPA) have the right to inspect and review the complete contents of their child's education record. It is the Organization’s responsibility to provide parents with access to this information as defined in their policies, as well as to define procedures for a parent, student, or staff member to challenge the accuracy of the information collected about them.

3. Reasonable Safeguards to Protect Confidentiality

Piano Marvel acknowledges that we have a responsibility to protect the confidentiality of personally identifiable information in our custody, throughout its entire lifecycle, using reasonable administrative, technical and physical safeguards associated with industry standards and best practices. Specific protection measures in use are described in Section III of this document.

4. Addressing Privacy Concerns and Complaints

Piano Marvel acknowledges that parents or eligible students have the right to have complaints about possible breaches of student data addressed. Complaints should be first directed to the appropriate Organization personnel as defined in their policies and the Organization’s published PBOR.

Clients may contact contactus@pianomarvel.com with any concerns about our privacy practices and data protection.

III. Protection of Personally Identifiable Student Information

A. Piano Marvel Security Strategy - Data Protection by Design and by Default

Piano Marvel systems are fully compliant with several comprehensive industry-recognized security standards. Significant overlap exists between the concepts of data security and data privacy; thus our approach to compliance has always been aimed at providing both, through multiple layers of controls designed to support our clients' defined policies. We ensure data security using a combination of Preventive, Detective, and Organizational controls, including network architecture and configuration, software design, policies, procedures and other critical protective measures.

1. How do we decide on reasonable safeguards for the protection of student data?

Piano Marvel continually reviews our existing safeguards to ensure that they are sufficient, using industry standard threat assessment and best practices. Because there is never a guarantee of 100% prevention, our program also includes Response and Recovery controls.

B. Infrastructure

Data protection starts with a secure infrastructure. All critical system components are housed in a secure data center, which provide assurance of physical and environmental security. SSH access to servers in this data center is strictly limited.

The Piano Marvel network is segmented to isolate highly sensitive data. Firewall rules are defined to explicitly allow specific types of traffic based on documented business and deny the rest by default. Rules are reviewed regularly by the technical team to ensure that only the necessary traffic is being allowed.

Data in transit on our network is protected by TLS protocol.

C. Data Storage and Protection

Sensitive data that requires special handling falls into several categories:

- PII of students - name, email address, username - subject to various privacy regulations, including
    - NY State Education Law Section 2-d
    - Georgia Student Data Privacy, Accessibility and Transparency Act
    - PPRA
    - COPPA
- Education records - subject to FERPA
- PII of staff - subject to various evolving privacy regulations

Student and staff data will be securely stored in a secure data center. Any access to this data by Piano Marvel requires an administrator login with strong password requirements and multi-factor authentication (MFA). Access is additionally protected by strict firewall rules.

Application code vulnerabilities can result in direct or indirect exposure of sensitive information. In order to prevent this, Piano Marvel applications are developed and tested in accordance with industry-recognized best practices.

- Separate Development/Test/Production environments to avoid the risk of introducing security flaws into live systems, and minimize exposure of sensitive data during development lifecycle
- Change control processes ensure that new code is tested and approved before being released
- Recently-modified code is regularly scanned and tested for vulnerabilities

All data transferred between the servers and the browser/client, including all pages on the Piano Marvel website, are encrypted with SSL technology.

D. Logical Access Control

Logical access control is governed by the principle of least privilege. Specific users are granted the minimum access needed to perform their job functions.

The following Piano Marvel staff members have access to education records as necessary to perform their job duties:

- Our client support team has administrator-level access to the applications in order to assist client users with technical issues.
- Only specific members of technical staff can access the database directly, by remotely connecting to servers via SSH. SSH access is only granted to those members who need it to perform their job functions, and is limited to specific servers/IP address ranges based on role. The access control list is reviewed by the Information Security team on a quarterly basis to determine whether access is still needed. Accounts are modified or disabled based upon changes in job responsibilities.

1. Application Access

Organization staff members may be granted access to view student PII within the Piano Marvel application. This requires the consent of the student.

Application user accounts may be created by Piano Marvel staff during the initial phase. Application accounts may also be created by Organization staff members or students.

In order to prevent unauthorized application access:

- Passwords are stored encrypted with a one way hash.
- Login attempts are rate-limited after multiple failed login attempts.
- Passwords cannot be retrieved, only changed to new passwords.

2. Tech Staff Access

Access to all servers is granted according to the principle of least privilege; that is, an individual is granted only the minimum privileges necessary to do their assigned job.

All members of the Piano Marvel development team require administrative access to the systems they develop and support. Developers have both privileged and non-privileged accounts where feasible, and only use the privileged accounts when performing specific functions that actually require administrative access.

Non-development staff will be granted privileges on an as-needed basis.

All Piano Marvel employee emails and accounts are secured with strong passwords and multi-factor authentication (MFA).

IV. Breach notification requirements

Should Piano Marvel become aware of any unauthorized release of student data, in violation of applicable privacy laws, the parents' bill of rights, and/or binding contractual obligations relating to data privacy and security, we will notify the Organization's designated privacy official in the most expedient way possible and without unreasonable delay.

If there is valid reason to suspect a breach (i.e., clients report fraudulent activity on their accounts, or we see signs that someone has gained unauthorized access to Piano Marvel's systems), Piano Marvel incident response team will:

- Check for common indicators of compromise to determine whether or not a breach has actually occurred.
- Notify management of findings.
- Conduct additional research as necessary to determine the extent of impact.

If it is determined that a breach has occurred, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.)