CONTRACT ADDENDUM
Protection of Student, Teacher, and Principal Personally Identifiable Information

1.   Applicability of This Addendum

The Delaware-Chenango-Madison-Otsego BOCES ("BOCES") and MakeMusic, Inc. ("Vendor") are parties to a contract dated July 1, 2024 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, MakeMusic Cloud ("Product"). BOCES's use of the Product results in Vendor receiving student personally identifiable information, or receiving teacher and principal personally identifiable information, as those terms are defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2.   Definitions

2.1   "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of Section 3012-c of the New York State Education Law, where that information is received by Vendor from BOCES or a Participating School District or is created by the Vendor's product or service in the course of being used by BOCES or a participating school district.

2.2   "Vendor" means MakeMusic, Inc.

2.3   "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Delaware-Chenango-Madison-Otsego BOCES and any school district or board of cooperative educational services that is a Participating School District under this Contract.

2.4   "BOCES" means the Delaware-Chenango-Madison-Otsego Board of Cooperative Educational Services.

2.5   "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6   "Parent's Bill of Rights" or "PBRDPS" means the Madison-Oneida BOCES Parents Bill of Rights for Data Privacy Security, a signed copy of which is included in Attachment A to this Addendum, and is incorporated into and made a part of this Data Security and Privacy Plan.

2.7   "Student" means any person attending or seeking to enroll in an educational agency.

2.8   "Eligible Student" means a student eighteen years or older.

2.9 "Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes the Delaware-Chenango-Madison-Otsego BOCES when it uses the Product to support its own educational programs or operations.

2.10 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.11 "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or any Participating School District, or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. **Ownership and Location of Protected Information**

   7.1   Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with the applicable Participating School District, and with BOCES to the extent that it acts on behalf of the Participating School District. Vendor shall acquire no ownership interest in education records or Protected Information.

   7.2   BOCES and a Participating School District shall have access to the Participating School District's Protected Information at all times through the term of this Contract. BOCES and a Participating School District shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

   7.3   Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or a Participating School District or their authorized users, or performing any other data analytics other than those required to provide the Product specified for a particular Participating School District in the applicable BOCES Purchase Order. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

   7.4   All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. **Purpose for Sharing Protected Information**

   The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES and Participating School Districts.

9. **Downstream Protections**

   Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. **Protected Information and Contract Termination**

    10.1   The expiration date of this Contract is defined by the underlying contract.

10.2   Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES or a Participating School District.

10.3   Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4   Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5   To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6   Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11.   Data Subject Request to Amend Protected Information

11.1   In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the student's district of enrollment for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2   In the event that a teacher or principal wishes to challenge the accuracy of Protected Information that qualifies as teacher or principal Protected Information for purposes of Education Law Section 2-d, that challenge shall be processed through the appeal process, if any, in the APPR Plan of the employing educational agency.

11.3   Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly with the data subject.

12.   Vendor Data Security and Privacy Plan

12.1   Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2   Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

i. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract, or BOCES or a Participating School District unless (1) Vendor has the prior written consent of the parent, eligible student, or teacher or principal to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than

the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4   Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5   Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6   Vendor will notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

13.7   Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES and any affected Participating School District for the full cost incurred by BOCES or the Participating School District to send notifications required by Education Law Section 2-d.

For Delaware-Chenango-Madison-Otsego BOCES   For MakeMusic, Inc.

Christopher Pany
2024.03.06
11:16:29 -07'00'

Name: Vanessa Warren   Name: Christopher Pany
President of the Board of Education   Contracts Manager

Date: 4/17/24   Date: 03/06/24

Attachment A – Parents' Bill of Rights for Data Security and Privacy

Delaware-Chenango-Madison-Otsego BOCES
Parent's Bill of Rights for Data Privacy and Security

DCMO BOCES Parents' Bill of Rights for Data Privacy and Security

DCMO BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our district and school operations.

DCMO BOCES seeks to insure that parents have information about how the District stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, DCMO BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 601. You may access this Policy from the District's website.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

For MakeMusic, Inc.

Christopher Pany
2024.03.06
11:16:39 -07'00'

Date: 03/06/24

Name: Christopher Pany
Title: Contracts Manager

Supplemental Information About This Contract

CONTRACTOR NAME	MakeMusic, Inc.
PRODUCT NAME	MakeMusic Cloud
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to BOCES and Participating School Districts. The product or services are used as an instructional music software and teaching tool
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.
DATA DESTRUCTION INFORMATION	The agreement expires June 30, 2025 Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES or a Participating School District. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the student's district of enrollment for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of Protected Information that qualifies as teacher or principal Protected Information for purposes of Education Law Section 2-d, that challenge shall be processed through the appeal process, if any, in the APPR Plan of the employing educational agency.
SECURITY PRACTICES	The data is stored in the continental United States (CONUS) or Canada. Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption,

	firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).

Attachment B – BOCES Applicable Policies

Policy #5304 "Information Security Breach"

Policy #5306 "Protection of Student Teacher and Principal Personal Information (Data Security and Privacy)

Policy #7500 Education Records

Attachment C – Vendor's Data Security and Privacy Plan

See summary document to follow

To follow is a summary accounting of our policies and procedures relating to data privacy and security. Further information regarding our policies and be found at the follow: for MakeMusic website and marketing, see the MakeMusic Privacy Statement; for **MakeMusic Cloud**, please see the specific **MakeMusic Cloud Privacy Policy** which governs the use of the application.

Purpose of Data Collection/Use:

We collect information to: (a) provide our Sites and Services; (b) provide information about our products and Services, such as updates and new features; (c) provide information about data security and privacy; (d) learn more about our customer's preferences; (e) enhance, personalize, and support your experience on our Sites and develop our products to better serve customer needs; and (f) monitor the success and/or usage of features to improve performance and functionality.

Data Accuracy/Corrective Practices:

Parents, eligible students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Subcontractor Oversight:

Individual subcontractors (personnel) receive the same training as employees and are bound by the same policies and agreements regarding handling customer data and PII.

MakeMusic Cloud Suprocessors (Service Providers):

In order to provide our users with the best experience possible, we use subprocessors and/or service providers to assist our efforts to analyze and improve our products, resolve errors or issues, and/or manage billing and accounting information. We send deletion requests to our subcontractors when we receive deletion requests from our customers to ensure data is deleted.

MakeMusic enters into data addendums and/or DPAs with subprocessors and service providers (subcontractors) as applicable to secure and protect data. All subprocessors and service providers are obliged to use any received data solely for the purposes outlined in our service agreements and to maintain industry standards safeguards and practices regarding data privacy and security.

The following subprocessors/service providers may, in the course of performing the agreed upon services, encounter customer data: Alfred Music, Asana, Atlassian, Avalara, AWS, Braintree, ConfigCat, Datadog, Fivetran, Global Grid for Learning, Google, Hubspot, Iterable, 84Codes, Maze, Microsoft, Netsuite, OneTrust, Peaksware, Redis, Rollbar, Salesforce, Satismeter, Sentry, Sigma, Snowflake, Survey Monkey, Twilio (Segment and Engage), Zendesk

Security Practices:

Data Storage:
- Customer data is securely housed in virtual machines and databases within the AWS us-east-1 region.

Protective Protocols:
- All traffic between users and the application occurs over HTTPS with TLS 1.2.
- Connections between application and database are encrypted using TLS.
- Application servers, database servers exist in a private virtual network.
- Network Security groups are used to restrict access to application/database servers.
- IAM policies are used to limit employee access to cloud computing resources.
- OS Security patches are installed in a timely manner.
- AWS GuardDuty is used to detect anomalous cloud account activity.
- Data is encrypted in transit and at rest at a minimum of 128-bit AES.
- Maintain a Data Incidence Response Plan which aligns with the NIST Cybersecurity Framework v1.1.
- Engage third-party vendors to perform penetration tests.
- Adopted practices and procedures which align with applicable NIST principles and industry-standard practices.
- Annual training for applicable employees and contracted personnel, covering:
    - FERPA law overview
    - COPPA law overview
    - Cybersecurity and best practices
    - State-specific requirements (as applicable)
    - Data security incident plans (for relevant employees)
    - How to handle requests for data access/erasure (for relevant employees)
    - How to verify identity for requests relating to customer data (for relevant employees)

Data Destruction:
Upon expiration of an agreement or termination of use, data may be securely destroyed or transferred, per and upon request from the EA or customer, barring any legal obligations.

Data Incident Response:
The following process will be followed when responding to a suspected incident:

1.Confirmed or suspected incidents shall be reported promptly to MakeMusic's engineering management at vhellot@makemusic.com or cpany@makemusic.com. A report will be filed that includes detailed information about the incident including team members involved, timelines, and data involved.
2. When an incident is reported, MakeMusic's engineering management will form a team with the necessary skills to investigate the severity of the incident, next steps, and potential remedies/solutions. Depending on the results of the investigation, MakeMusic's engineering management will determine if the incident constitutes a breach.

3. All investigations will be documented to ensure appropriate steps are taken and that consistency in response, management, and reporting is followed. MakeMusic's engineering management will communicate any updates to all other departments and stakeholders.

4. If it is determined a Data Breach has occurred per legal definition, MakeMusic shall implement the recovery and respond portion of its Data Incident Response plan and notify affected parties duly per legal requirement.

The objective of our incident response plan is to ensure that: a) a culture of vigilance is built and maintained; b) a framework exists to help expedite incident investigation; c) incidents are reported in a timely manner and can be properly investigated; d) incidents are handled by appropriately authorized and skilled personnel; e) the appropriate levels of management are involved in response; f) incidents are recorded and documented; g) organizational impacts are understood; h) action is taken to prevent further damage; i) evidence is gathered, recorded, and maintained during the process; j) customers, proper agencies, and affected parties are notified per legal statues and as appropriate; k) incidents are resolved in a timely manner; and l) Incidents are reviewed to identify improvements.

Privacy – Data Access Request:
Steps for how we handle requests for customer data access:
1. Ensure the request is captured in a Zendesk ticket or email to privacy@makemusic.com. Documentation is the first step in safety for our company and the customer.
2. Verify the customer's account exists. We first work to verify the request is coming from the account holder before proceeding with the request.
3. Ensure the information on the customer's account matches the information the customer wants to view/change. (E.g., johndoe@makemusic.com wants to view and/or edit John Doe's data, not John Smith's data. If the customer is a parent and the data does not match, we may be able to honor the request through the affiliate school or educational organization. If it is a school/admin wanting to view and/or alter information about a student or view/alter information about a child on the school's or a parent's behalf, we ensure they can provide the correct student information (first name, last name, email address) and that the student is a member of the platform associated with the person making the request.

MAKEMUSIC CLOUD PRICING

Standard Pricing

Subscription Type	Unit Price	Bulk Price Discount*
Teacher Subscription (*per Teacher*) Teachers may access the entire repertoire library, including over 13,000 digital sheet music titles and all of our teaching tools.	$59.99 *(annually)*	**$39.99*** 33% off (annually)
Student Subscription (*per Student*) Students may enjoy unlimited access to the entire repertoire library and practice tools.	$29.99 *(annually)*	**$13.99*** 53% off (annually)
Print Add-On (*per subscription*) Print add-ons are only available for orders with a minimum of 20 subscriptions and must be purchased for a minimum of 20 users.	n/a	**$15.99*** (annually)

Multi-Year Commitment** Pricing

Subscription Type	Bulk Price Discount*	2-Yr Commit	3-Yr Commit
Teacher Subscription (*per Teacher*) Teachers may access the entire repertoire library, including over 13,000 digital sheet music titles and all of our teaching tools.	$39.99* *(annually)*	**$33.99**** 15% off (annually)	**$29.99**** 25% off (annually)
Student Subscription (*per Student*) Students may enjoy unlimited access to the entire repertoire library and practice tools.	$13.99* *(annually)*	**$11.89**** 15% off (annually)	**$10.49**** 25% off (annually)
Print Add-On (*per subscription*) Print add-ons are only available for orders with a minimum of 20 subscriptions and must be purchased for a minimum of 20 users.	$15.99* *(annually)*	**$13.59**** 15% off (annually)	**$11.99**** 25% off (annually)

Pricing Notes:

*requires a minimum of 20 total subscriptions purchased of any combination (example: 1 teacher, 19 students; 19 teachers, 1 students; 5 teachers, 15 students; etc.)

A multi-year commitment discount is a reduced price for customers who commit to purchasing annual subscriptions for the chosen multi-year period. See **MakeMusic Cloud Terms of Service for additional terms. Similar to bulk discounts, it also requires a minimum of 20 total subscriptions purchased of any combination (example: 1 teacher, 19 students; 19 teachers, 1 students; 5 teachers, 15 students; etc.)