Supplemental Information for Agreement with MakeMusic Inc. (hereinafter "Third-party Contractor"): For purposes of further ensuring confidentiality and security of student data, each contract ("Agreement") the Mineola Union Free School District (the "District") enters into with a third-party contractor (the "Third-party Contractor") shall include a Data Security and Privacy Plan that includes a signed copy of the District's Parents' Bill of Rights and in which Plan the Third-party Contractor agrees to abide by the District's Parents' Bill of Rights and to comply with the following:

1) **Exclusive Purposes for which Student Data Will Be Used.** Use of Personally Identifiable Information ("PII") under the Agreement will be limited to that necessary for the Third-party Contractor to perform the duties outlined in the Agreement and the services associated with that function. The Third-party Contractor further agrees that no PII will be sold or used for marketing or commercial purposes.

2) **Protective Measures Regarding Third Parties.** The Third-party Contractor will ensure that any subcontractor or other person or entity with whom the Contractor shares student data and/or teacher or principal data, if applicable, agrees to abide by all of the components of applicable state and federal law, including New York Education Law Section 2-d, the District's Parents' Bill of Rights, and the Family Educational Rights and Privacy Act ("FERPA"). In addition, the Third-party Contractor will ensure that each subcontractor, person or entity with whom the Third-party Contractor shares student data and/or teacher or principal data will abide by all the terms and conditions of this Data Security and Privacy Plan.

3) **Expiration of Agreement.** Absent renewal, the Agreement expires annually on June 30th. If the District does not renew the Agreement past June 30th of the contractual year, all student data shall be deleted, within 90 days, in accordance with the National Institute of Standards and Technology (NIST) standard 800-88. The Third-party Contractor will ensure, at the sole discretion of the District, that all student data are returned to the District or provide confirmation to the District that the data in its possession has been securely destroyed. The Third-party Contractor will also ensure that all emails containing personally identifiable student information are returned to the District and deleted from the Third-party Contractor's email account. Third-party Contractor shall ensure that any data it retains after 90 days is data it is required to retain by law and retention is secured in accordance with NIST and/or HIPPA standards.

4) **Challenge to Accuracy of Data.** A parent, student, teacher or principal can challenge the accuracy of the Data received or generated by the Third-party Contractor in writing addressed to Whittney Smith, Ed.D., Director of Instructional Technology and Assessment, Mineola Union Free School District, 2400 Jericho Turnpike, Garden City Park, New York 11040.

5) **Storage of Data.** Student data shall be stored in a secure data center using monitoring of the access doors, fire and security monitoring, system health and intrusion monitoring, data backups and retentions. Data storage and access shall

comply with the Advanced Encryption Standard (AES) with minimum of 128 bit key encryption or better.

6) **Breach of Personally Identifiable Information.** The Third-party Contractor must notify the District of any breach or unauthorized release of PII within seven (7) calendar days of any such breach or Third-party Contractor's knowledge of such breach. The Third-party Contractor shall promptly reimburse the District and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of PII by the Third-party Contractor, its subcontractors, and/or assignees.

MINEOLA UNION FREE SCHOOL DISTRICT	THIRD-PARTY CONTRACTOR
By: _____	By: _____
Name: Cheryl Lampasona	Name: Christopher Pany_
Title: President, Board of Education	Title: ___Contracts Manager__

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.

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.

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 at rest at a minimum of 128-bit AES.
- Data is encrypted in transit 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.
- 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 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.