BRIARCLIFF MANOR UNION FREE SCHOOL DISTRICT
District Office
45 Ingham Road
Briarcliff Manor, New York 10510

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Briarcliff Manor UFSD Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
BRIARCLIFF MANOR UFSD and Make Music - SmartMusic

1. **Purpose**

(a) BRIARCLIFF MANOR UFSD (hereinafter "District") and Make Music - SmartMusic (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement").

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between BRIARCLIFF MANOR UFSD and Make Music - SmartMusic that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational, and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between BRIARCLIFF MANOR UFSD

and Make Music - SmartMusic." Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting the Data Privacy Officer, Erica Beasley directly by email at ebeasley@briarcliffschools.org or by calling (914) 432-8121.

(c) Vendor will cooperate with the District and provide as much information as possible directly to the Data Privacy Officer, Erica Beasley or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform the Data Privacy Officer, Erica Beasley or her designee.

6. **Additional Statutory and Regulatory Obligations** [1]

[1] Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

BRIARCLIFF MANOR UNION FREE SCHOOL DISTRICT
District Office
45 Ingham Road
Briarcliff Manor, New York 10510

Bill of Rights for Data Security and Privacy

BRIARCLIFF MANOR UFSD

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-c and 2-d of the Education Law, parents and students are entitled to certain protections regarding confidential student information. The Putnam/Northern Westchester B.O.C.E.S.is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below:

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.
3. The District is committed to implementing safeguards associated with industry standards and best practices under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the NYS Education Department, Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Data Privacy Officer, Erica Beasley, ebeasley@briarcliffschools.org, (914) 432-8121, 45 Ingham Road, Briarcliff Manor, NY 10510.
6. The District has entered into contracts with certain third-party contractors ("TPC") who have been sent personally identifiable student data as defined in 34 C.F.R. §99.3 and/or personally identifying teacher and/or principal data as defined by Education Law §3012-c(10). The following information about such contractors appears in such supplemental information to this document for each contract with a TPC, as required by law:
    - The exclusive purposes for which the student or teacher or principal data will be used by the TPC, as defined in the contract;
    - How the TPC will ensure that its subcontractors or other authorized individuals who will be in receipt of the data will abide by the applicable data privacy and security requirements of the federal and state laws and regulations (e.g., FERPA; Education Law §2-d);
    - The duration of the contract that sets forth its expiration date and description of what will be done with the data upon the expiration of the contract (e.g. whether, when and in what format the data will be returned to the educational agency or destroyed); and
    - If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the data that is collected.
7. Educational agency workers that handle personally identifiable information will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect such information.

8. Agreements with third-party contractors/consultants will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

9. A parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected by filing a written request with the District Superintendent of Schools or his administrative designee, Erica Beasley, Director of Technology, ebeasley@briarcliffschools.org

BRIARCLIFF MANOR UNION FREE SCHOOL DISTRICT
District Office
45 Ingham Road
Briarcliff Manor, New York 10510

Supplemental Information about a Master Agreement between

BRIARCLIFF MANOR UFSD and Make Music - SmartMusic [2]

BRIARCLIFF MANOR UFSD has entered into a Master Agreement with Make Music - SmartMusic, which governs the availability to the District of the following products or services:

SMART Music

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").
Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.
Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.
Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences on July 1, 2020 and expires on termination of agreement.
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will

[2] Each educational agency, including a school district, is required to publish a "Bill of Rights for Data Security and Privacy" on its website. *See*, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district's website] must also include "supplemental information" for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. *See*, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website *in their entirety*. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the "supplemental information" about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of "supplemental information" within each applicable contract, and have complied with the obligation to include the "supplemental information" for each applicable contract with their Bill of Rights, by posting *the text from this page of this Exhibit* from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

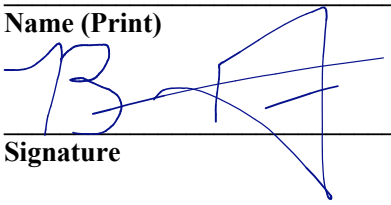
Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

BY THE VENDOR:

Brian Gruber

Name (Print)



Signature

Senior Manger, Sales

Title

11/10/2020

Date