

OREGON STUDENT DATA PRIVACY AGREEMENT
Version 2.0 (June 30, 2019)

and

This Oregon Student Data Privacy Agreement ("DPA") is entered into by and between the
(hereinafter referred to as "LEA") and
(hereinafter referred to as "Provider") on . The Parties agree to the terms as
stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state student privacy laws, including SB 187, Oregon Student Information Protection Act ("OSIPA"), Or. Rev. Stat. § 646.607 – 646.652; Or. Rev. Stat. § 326.565, et seq. (Student Records); and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in Oregon the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, OSIPA and other applicable Oregon State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.
2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

3. **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”:
4. **DPA Definitions**. The definition of terms used in this DPA are found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer student-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data on the student’s records, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account**. If student Generated Content is stored or maintained by the Provider as part of the Services described in Article I, section 2 and/or Exhibit “A”, Provider shall, at the request of the LEA, transfer said Student Generated Content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.
4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited. The Provider shall not use, disclose, compile, transfer, sell the Student Data, Student Generated Content and/or any portion thereof to any third party or other entity or allow any other

third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof.

5. **No Unauthorized Use**. Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (34 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes.
2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR § 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Directive for Disposition of Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.
 - a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.

 - b. **Complete Disposal Upon Termination of Service Agreement.** Upon termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from

using Student Data for adaptive learning or customized student learning purposes, as long as such learning purposes are available for use by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks in compliance with state and local ordinances.
 - b. **Destruction of Data.** Data shall be destroyed and disposed as defined above in Article IV, section 5.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
 - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
 - e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the Service Agreement.
 - g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the

terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:
- a. The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
 - b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - c. At LEA’s discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - d. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of

any such data breach.

- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA request Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate this DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article IV, section 5.
4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other agreement resulting from a solicitation, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives below:

a. Designated Representatives

The designated representative for the **Provider** for this Agreement is:

Name: _____
Title: _____
Email: _____
Phone: _____

The designated representative for the **LEA** for this Agreement is:

Name: _____
Title: _____
Email: _____
Phone: _____

b. Notification of Acceptance of General Offer of Privacy Terms. Upon execution of Exhibit E, General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: _____
Title: _____
Email: _____
Phone: _____

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
8. **Governing Law: Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof is stored, maintained or used in any way.
10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. Each party agrees to make this DPA part of and explicitly annotated in any agreement which forms a successor entity.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Oregon Student Data Privacy Agreement as of the last day noted below.

Enter the Provider's Name

BY: BAF Date: _____

Printed Name: _____ Title/Position: _____

Address for Notice Purposes:

BY: Megan Nace Date: _____

Printed Name: _____ Title/Position: _____

Address for Notice Purposes:

EXHIBIT “A”

DESCRIPTION OF SERVICES

- **Users with premium subscriptions can print thousands of titles from key music education publishers.**
- **Students see which notes and rhythms they played correctly/incorrectly, receive a performance score, and hear their recording.**
- **SmartMusic’s content library that includes 150+ method books, 5,400+ ensemble titles and thousands of solos from top publishers.**
- **A metronome, tuner, and the ability to loop sections are built in and always close at hand.**
- **Both teachers and students can see each others’ written comments on every assignment and student recording.**
- **Teachers can instantly create an unlimited number of sight-reading exercises for any type of ensemble or individual instrument.**
- **Provide students with a sense of how their part fits in and an opportunity to model their performances after world-class musicians.**
- **Create your own custom notation as well as import and export MusicXML files between most popular music notation products.**
- **Teachers using the Compose notation tool, share your compositions privately and publicly with your performers.**
- **Track student progress in SmartMusic’s online Gradebook, accessing student recordings, assignments, and performance scores.**
- **Customize rubrics with the criteria that matters for your curriculum.**
- **Collect assignments into units, and easily assign those units to multiple classes.**
- **Track student practice time – down to the second – as it happens.**
- **SmartMusic works on the devices your students use today, including computers, Chromebooks, and iPads.**
- **Colors adjusted to ensure that people who see colors differently have equal access.**

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.	✓ Details listed under "Other"
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	All data usage related information can be referenced under Exhibit F below.
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	Assessments through sound recordings occur within the SmartMusic application, saved, and send to the teacher's gradebook with the application.
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	Within the application assignments are received by the student from the teacher, assignments are completed by the student and transferred back to the teacher. Other types of communications that are sent are emails for the purpose of password reset, account verification, and receipt emails for purchases.

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
Enrollment	Other demographic information- Please specify:	
	Student school enrollment	<small>Students are enrolled in courses via invitation links from their teachers.</small>
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information- Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses	Students are enrolled in courses via invitation links from their teachers.
	Teacher names	Teacher names are stored in their personal accounts and appear in the class settings.
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	Students are connected to their schools or districts by email invitations sent by the teacher, owner, or administrator of the account.

	number	
	State ID number	
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓ Passwords are encrypted
Student Name	First and/or Last	Students' first and last name are stored on their personal accounts.
Student In App Performance	Program/appli- cation performance (typing program-student types 60 wpm, reading program-student reads below grade level)	Within the application assignments are received by the student from the teacher, and assessments are sent back to the teacher.
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:	Within the application assignments are received by the student from the teacher, and assessments are sent back to the teacher. Practice time is also recorded in the application.
Transcript	Student course grades	Student grades can be recorded by the teacher in the gradebook portion of the application.
	Student course data	Student practice time is recorded within the application, and can be viewed by the student and the teacher of their course.
	Student course grades/performance scores	Student grades can be recorded by the teacher in the gradebook portion of the application.
	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	

No Student Data Collected at this time _____.
 *Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space needed.

New SmartMusic cookie names and details can be found at <https://wpmedia.makemusic.com/wp-content/uploads/2019/10/new-SmartMusic-Privacy-Policy-10-29.pdf>

EXHIBIT “C”

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the states of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Covered Information: Covered Information means materials that regard a student that are in any media or format and includes materials as identified by Oregon SB 187 (2015). The categories of Covered Information under Oregon law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or student-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. Within the DPA the term "Provider" includes the term “Third Party” as used in applicable state statutes.

Student Generated Content: The term “student-generated content” means materials or content created by a student during and for the purpose of education including, but not limited to, essays, research

reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

Student Records: Means both of the following: (1) Any information that directly relates to a student that is maintained by LEA and (2) any information acquired directly from the student through the use of instructional software or applications assigned to the student by a teacher or other LEA employee. For the purposes of this Agreement, Student Records shall be the same as Educational Records, and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; and (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. Student Data shall constitute Student Records for the purposes of this Agreement, and for the purposes of Oregon and Federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated

content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] (LEA) directs [Name of Company] (Provider) to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

___ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

___ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

3. Timing of Disposition

Data shall be disposed of by the following date:

___ As soon as commercially practicable

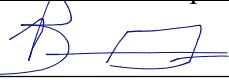
___ By

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data



Authorized Representative of Company

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

(hereinafter referred to as "Provider") Provider offers the same privacy protections found in this DPA between it and _____ (hereinafter referred to as "LEA") and which is dated _____ to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by the LEA to the Provider in Exhibit "B" to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the LEA's originating Service Agreement; or (3) three (3) years after the date of Provider's signature to this Form. Provider shall notify either the ACPE or SDPC in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

BY:  _____
Brian Gruber

Date: _____

Printed Name: _____

Title/Position: _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____

Date: _____

Printed Name: _____

Title/Position _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

New SmartMusic Data Privacy Policy
LAST UPDATED ON OCTOBER 29th, 2019.

Information You Give Us

Contact Information: You give us your Contact Information when you request information, register with or subscribe to the Site. “Contact Information” includes your name, email, company, address and/or telephone number.

We may use your contact Information and other Personal Data to:

Provide you the Services on the Site;

Fulfil your requests for information; and

Contact you about MakeMusic, Inc. products or services based on the preferences you have indicated. Personal information we collect is used to provide, maintain, and improve our Services.

We use information about how you use our website to offer you custom content, such as music searches targeted to your selected instrument or how many times you open a piece of content, so we can tailor our Services to your preferences. We also use your data to maintain our applications, so they continue to serve the needs of the customers.

We may use your email address to send you information about changes or improvements we are making. Users meeting the age to legally consent to sharing their personal information online per their country/territory law may opt into MakeMusic marketing promotions.

We may store personal information such as name, address, school or district name, purchase order numbers, or credit card information for Schools or individuals over the age of 13 (United States and Canada) or 16 (European Union) that purchase a SmartMusic subscription. Credit card information is encrypted and transferred using secure Hypertext Transfer Protocol (HTTPS).

We may use personal information to contact an individual regarding an account issue via telephone, fax, email, or written correspondence.

When you visit our Help Center, we may collect your name or email address(es) and associate them with a case number so that we can respond to inquiries and requests.

We may use Non-Personally Identifiable User Information several ways and for several purposes, including (without limitation):

To calculate necessary royalty payments to third party content providers, which are often based on the number of times a work is opened or accessed by our users.

To prepare reports and other materials that we may share with others in an anonymous format.

For analytics purposes.

In some instances, we use third-party vendors to collect, monitor and/or maintain Non-PII. For example: In our web applications we utilize Rollbar and Google and Google Analytics. Rollbar is utilized for error monitoring. Information logged includes common request data. Google Analytics is utilized to analyse application, feature and content usage.

A detailed list of information you may give us:

Districts, Platform Owners, Platform Administrators, and Teachers:

First Name, Last Name
Email Address
Username
Country
Timezone
Marketing preferences
Address
Phone number
Fax number
Instrument played
District, School or Studio name
Physical Address
Billing Address
State
Phone number
Class Name
Sales Order information
Password

Students:

First Name
Last Name
Email address
Username
Country
Timezone
Instrument(s) played
Password

Parents:

First Name
Last Name
Email
Address
Phone number
Payment information (Encrypted Credit Card)

Information We Collect from You

We collect Analytical Information through automated means when use and navigate the Sites. “Analytical Information” includes pages and products viewed, emails from us that you opened, browser type, operating system, IP address and device information, your mobile operating system (OS), a mobile device identifier embedded by us, or other commonly used mobile device identifier if you access the Sites on a mobile device.

We use Analytical Information to:

Retain and evaluate information from your visits to the website and how you move around for analytics purposes to improve our website to make it more user friendly or improve the speed of the page loading or the website in general.

Review user preferences when navigating the site and to develop new services that may be able to better appeal to our customers based upon what information our customers view or how they navigate the website;

Specific information collected:

We collect information about how and when you use SmartMusic (i.e. when you submit an assignment, what kind of music you search for, or when you create a class). This information includes:

Personal Identifier (Id number). This is a unique number our Services assigns to your account upon creation.

Log data. When you use SmartMusic, we automatically record and store particular information in our server log files. This data may include:

Device Information

IP Address

Browser

OS

Hardware model

Mobile network information

The date and time the Services were used

Communications

We log communications history in order to resolve any issues or respond to requests.

We may use your email address to inform you of any changes or improvements MakeMusic will be making.

We do not send promotions to users under the age of 13 (United States and Canada) or 16 (European Union).

Additional information collected:

Platform ID - a unique number our Services assigns to a platform (school, district) upon creation.

Musical recordings

Grades

Notes

Time practiced

Anonymized usage on features and music opened

5. Information we obtain from others. We may also collect publicly available information about you from third-party sources, such as the postal service for shipping address verification.

6. Information We Share. Your information will be visible to owners, administrators, and if applicable, your teacher(s) within your Platform. Users are invited to the Platform and managed by Platform owners and administrators.

3. Cookies

You may be aware that there is a technology called “cookies”. For the purposes of this Privacy and Cookies Statement, cookies include similar technologies, for example clear gifs, internet tag technologies, web beacons, and embedded scripts. These are small text files that are transferred from the website to the hard drive of your computer. We use cookies to enable the website to work more efficiently and to provide us with information about your activities on the website.

Our cookies will not allow us to obtain information of a personal nature that will identify you to us, such as your name and address. We will only be aware of such information if you provide the information to us, or you have set the preferences in your browser to provide this information automatically.

Details of the cookies we use are as follows:

Strictly Necessary Cookies: These cookies are essential in order to enable you to move around the website and use its features. Without these cookies the services you have asked for, such as tutorials, cannot be provided.

Performance Cookies: These cookies collect information about how visitors use a website, for instance which pages visitors go to most often. These cookies do not collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how the website works. By using our website, you agree that we can place these types of cookies on your device.

Functionality Cookies: These cookies allow the website to remember choices you make and provide enhanced, more personal features. For instance, these cookies can be used to remember the volume level you prefer to use when watching videos on our website. The information these cookies collect may be anonymized and they cannot track your browsing activity on other websites.

Targeting cookies: We do not use targeting cookies within the SmartMusic web application.

By using our website or otherwise clicking on the “Accept” button of our cookies notice, you agree that we can place these types of cookies on your device.

Your web browser may allow some control of most cookies through your browser settings. To find out more about cookies, including how to see what cookies have been set on your computer and how to manage and delete them, visit www.allaboutcookies.org. Please note that you may delete and block all cookies used by this website, but if you do so parts of the website may not work.

New SmartMusic cookie names and details can be found at <https://wpmedia.makemusic.com/wp-content/uploads/2019/10/new-SmartMusic-Privacy-Policy-10-29.pdf>

4. External processing:

In order to provide our users with the best experience possible, we use subprocessor tools in order to analyze and improve our products, resolve errors or issues, or manage billing and accounting information.

Third Parties used by new SmartMusic can be found at <https://wpmedia.makemusic.com/wp-content/uploads/2019/10/new-SmartMusic-Privacy-Policy-10-29.pdf>

Data retention

Because we can not predict the exact date or time a customer chooses to stop using our services or products, MakeMusic retains data only as long as necessary as determined by their customers. Data will be deleted upon request.

Age Limitations. We care about protecting the online privacy of children. We may collect certain information about children ONLY for the purpose of providing our educational Services as described in the sections above regarding enrollment information.

Verifiable Consent. MakeMusic does not knowingly collect any information from children under the age of 13 (United States and Canada) or 16 (European Union) unless the school or teacher has obtained appropriate, verifiable consent directly from the parent or legal guardian for the student to use the Services. It is the responsibility of the school or teacher to obtain and verify consent from a parent or legal guardian in order for any child under 13 years of age (United States and Canada) or 16 (European Union) to use the Services.

Notification. The school remains responsible for obtaining verifiable consent for its students under the age of 13 (United States and Canada) or 16 (European Union). The new web-based SmartMusic service will only allow students under the age of 13 (United States and Canada) or 16 (European Union) to access the SmartMusic service via a class code provided by their teacher who has obtained parental consent on behalf of the student to use the SmartMusic service or by consent of a parent via a credit card purchase.

Providing or Withdrawing Consent. If, as a parent or legal guardian, you have not received information from your school, please contact the teacher or school directly. If you have received notice from the school and have not given your consent, or if you believe we have inadvertently collected personal information of a child under 13 (United States and Canada) or 16 (European Union) without proper parental consent, please contact us directly so that we may delete such data as soon as possible; contact information can be found at the bottom of this document. You should, at a minimum, clearly state: (i) the name of the child, along with their username; (ii) age and birth date of the child; (iii) your relationship to the child (e.g., parent, guardian, teacher); (iv) as much detail as possible regarding the information you believe was provided improperly by the child. After confirming your identity, we will provide you with an opportunity to review, and if you wish, delete such information.

Review Rights. If you are a parent/guardian and wish to review information submitted by your child, you may contact us (contact information is set forth below) and, after confirming your identity, we will provide you with an opportunity to review, and if you wish to delete such information.

6. Your Ability to Modify Our Use of Your Personal Data

You have the following rights related to MakeMusic's use of your Personal Data:

Number

Description of your right

Right 1

A right to access personal data held by us about you, as well as information about how we are using your data.

Right 2

A right to require us to rectify any inaccurate personal data held by us about you.

Right 3

A right to require us to erase personal data held by us about you, and where the personal data has been made public, for other controllers processing the personal data to also erase links to, or copy or replication of such personal data. This right will only apply where (for example): we no longer need to use the personal data to achieve the purpose we collected it for; or where you withdraw your consent if we are using your personal data based on your consent; or where you object to the way we process your data (in line with Right 6 below).

Right 4

A right to restrict our processing of personal data held by us about you. This right will only apply where (for example): you dispute the accuracy of the personal data held by us; or where you would have the right to require us to erase the personal data but would prefer that our processing is restricted instead; or where we no longer need to use the personal data to achieve the purpose we collected it for, but you require the data for the purposes of dealing with legal claims.

Right 5

A right to receive personal data, which you have provided to us, in a structured, commonly used and machine-readable format. You also have the right to require us to transfer this personal data to another organisation, at your request.

Right 6

A right to object to our processing of personal data held by us about you (including for the purposes of sending marketing materials to you).

Right 7

A right to withdraw your consent, where we are relying on it to use your personal data (for example, to provide you with marketing information about our services or products).

If you have consented to receive communications from us, you can contact us at any time to have your details removed from lists used by us or to update your marketing preferences. Please email team@makemusic.com and quote your email/telephone number/account number in the body of the email, telling us what you would like us to do.

You can also: click "unsubscribe" on any of our emails, and we will ensure we don't send you any communications of this nature in the future.

To exercise any of your rights above, please contact MakeMusic at:

privacy@makemusic.com

and/or

MakeMusic, Inc.

7007 Winchester Circle, Suite 140

Boulder, CO 80301, United States.

If you choose to exercise any of your rights listed above, it may affect your ability to use the Site, as the operation and functionalities provided on the Site may require the use of your Personal Data.

7. Security

We will take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction of your Personal Data, taking into due account the risks involved in the processing and the nature of the personal data. However, no electronic storage method or data transmission over the Internet can be guaranteed to be 100% secure.

8. Policies of Other Websites

The Site may contain links to third-party websites not owned or controlled by MakeMusic, Inc. MakeMusic, Inc. is not responsible for the privacy policies of any third-party websites which a user may access through a third-party link. Further, these third-party websites may have privacy policies that differ from this Privacy Policy. MakeMusic, Inc. disclaims all responsibility for the privacy practices of such other third-party websites. You should read the privacy policies of each third-party website you visit to determine what information each third-party website may be collecting about you and how they intend to use such information.

9. Contact us

If you have any questions or comments about these Terms of Use or this Site, please contact us by email at privacy@makemusic.com. You may send us a letter addressed by First Class Postage Prepaid U.S. Mail or overnight courier to the following address:

MakeMusic, Inc.
Attn: Customer Success MakeMusic, Inc.
7007 Winchester Circle, Suite 140 Boulder, CO 80301
United States of America

- Visit us at support.makemusic.com
- Call us toll free (for the U.S.A.): 1-800-843-2066 | International callers: (952) 937-9611

If you have any concerns regarding our processing of your personal information or are not satisfied with our handling of any request by you in relation to your rights, please get in touch with our Customer Success team at the contact details set out below in the first instance. You always have the right to make a complaint to the Information Commissioner's Office ("ICO"). The ICO is the UK's independent body set up to uphold information rights. You can find out more about the ICO on its website (<https://ico.org.uk/>). Their address is:

First Contact Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF