OREGON STUDENT DATA PRIVACY AGREEMENT Version 1.0

Beaverton School District

and

Spotify USA Inc.

5/11/2019 (Date)

This Oregon Student Data Privacy Agreement ("DPA") is entered into by and between the Beaverton School District (hereinafter referred to as “LEA”) and Spotify USA Inc.(hereinafter referred to as “Provider”) on 5/11/2019. 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 5/11/2019 (“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 Federal 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**, this Agreement complies Oregon laws and Federal Law.

**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", 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 state privacy 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.

**2. Nature of Services Provided**.

The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit “A” here to:

Soundtrap is an easy-to-use, online audio recording studio. Students and teachers can collaborate in a safe classroom, using any device, at any time from any location! While harnessing critical thinking and communication skills through collaborative, creative audio recording projects, Soundtrap bridges the necessary skills for preparing our 21st century learners for a global, connected world.

**3. Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit “B”:

See Exhibit B

**4. DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term 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 pupil-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 pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil 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**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

**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 will not use, disclose, compile, transfer, sell the Student Data 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 no less protective than the terms of this DPA.

## ARTICLE III: DUTIES OF LEA

**1. Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes quoted in this DPA.

**2. Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 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, and determine whether Provider qualifies as a school official.

**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 identified in this DPA.

**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.

**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. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to 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 **Beaverton School District** 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**. Provider shall upon request 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 and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. 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. 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. Provider shall upon request 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, (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 as soon as possible after receipt of said request.

**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 Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client. This section does not prohibit Provider from generating legitimate personalized learning recommendations.

## 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 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 the background checks of the Provider.

**b. Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

**c. Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices 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 computer environment and not copy, reproduce, or transmit 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, Secure Socket Layer ("SSL") or equivalent technology shall be employed 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**. 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 remain responsible for the processing of Data by its Subprocessors.

**h. Periodic Risk Assessment**. Provider further acknowledges and agrees to

conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

**i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

**j. Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to reasonably audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof. The Provider will cooperate as commercially reasonable with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider.

**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. 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.** At the request and with the assistance of LEA, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

## ARTICLE VI- GENERAL OFFER OF 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 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. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for a period of three (3) years, or so long as the Provider performs services under this Agreement, whichever shall be longer.

**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.

**3. Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

**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 identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, 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, facsimile 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: The designated representative for the Provider for this Agreement is:

_____

The designated representative for the LEA for this Agreement is:

_____

**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 PERFORMED, 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.

[*Signature Page Follows*]

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

Spotify USA Inc.
BY: Dominik Sanya Date: 5/11/2019

Printed Name: Dominik Sanya Title/Position: Global Head of Creator Marketing

Address for Notice Purposes:
Spotify USA Inc.
150 Greenwich St.
62nd Floor
New York, NY 10007

Beaverton School District

BY:_____ Date:_____

Printed Name:_____ Title/Position:_____

Address for Notice Purposes:
_____

## EXHIBIT “A”

Soundtrap is an easy-to-use, online audio recording studio. Students and teachers can collaborate in a safe classroom, using any device, at any time from any location! While harnessing critical thinking and communication skills through collaborative, creative audio recording projects, Soundtrap bridges the necessary skills for preparing our 21st century learners for a global, connected world.

# 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. | ✔ |
| | Other application technology meta data-Please specify: | |
| | | |
| Application Use Statistics | Meta data on user interaction with application | ✔ |
| | | |
| Assessment | Standardized test scores | |
| | Observation data | |
| | Other assessment data-Please specify: | |
| | | |
| Attendance | Student school (daily) attendance data | |
| | Student class attendance data | |
| | | |
| Communications | Online communications that are captured (emails, blog entries) | ✔ |
| | | |
| 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) | ✔ |
| | Other demographic information-Please specify: | |
| Enrollment | Student school enrollment | |
| | 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 | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| | | |
| | | |
| Schedule | Student scheduled courses | |
| | Teacher names | ✔ |
| | | |
| Special Indicator | English language learner information | |
| | Low income status | |
| | Medical alerts | |
| | Student disability information | |
| | Specialized education services (IEP or 504) | |
| | Living situations (homeless/foster care) | |
| | Other indicator information-Please specify: | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Student Contact Information | Address | |
| | Email | ✔ |
| | Phone | |
| | | |
| Student Identifiers | Local (School district) ID number | |
| | State ID number | |
| | Vendor/App assigned student ID number | |
| | Student app username | |
| | Student app passwords | |
| | | |
| Student Name | First and/or Last | ✔ |
| | | |
| Student In App Performance | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | |
| | | |
| 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. | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Other | Other student work data - Please specify: | |
| | | |
| Transcript | Student course grades | |
| | Student course data | |
| | Student course grades/performance scores | |
| | Other transcript data -Please specify: | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| 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 | |

**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, and test protocols. 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 800-63-3**: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

**Operator:** The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statues.

**Personally Identifiable Information (PII):** The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-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 pupil records. Within the DPA the term "Provider" includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Pupil Generated Content:** The term “pupil-generated content” means materials or content created by a pupil 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 pupil content.

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

**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 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 Pupil 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.

**Student Personal Information:** "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student. For purposes of this DPA, Student Personal Information is referred to as Student Data.

**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 pupil 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] directs Spotify USA Inc. to dispose of data obtained by Company pursuant to the terms of the Service Agreement between LEA and Company. 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

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

2. Nature of Disposition

__X__ 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: Insert Special Instructions

3. Timing of Disposition

Data shall be disposed of by the following date:

__X__ As soon as commercially practicable

_____By

4. Signature

_____ Authorized Representative of LEA

_____ Date

5. Verification of Disposition of Data

Dominik Sanya_____ Authorized Representative of Company

5/11/2019_____ Date

**EXHIBIT "E"**
GENERAL OFFER OF PRIVACY TERMS

**1. Offer of Terms**
Provider offers the same privacy protections found in this DPA between it and Beaverton School District and which is dated 5/11/2019
to any other LEA ("Subscribing LEA") who accepts this General Offer though 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 Subscribing LEA to the Provider 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 Originating Service Agreement; or 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: Spotify USA Inc.
Date: 5/11/2019
Printed Name: Dominik Sanya
Title/Position: Global Head of Creator Marketing

**2. Subscribing LEA**
Beaverton School District

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: Beaverton School District
Date:_____
Printed Name:_____
Title/Position_____

## EXHIBIT "F" DATA SECURITY REQUIREMENTS

Insert additional data security requirements

**Signature:** Dominik Sanya
Dominik Sanya (May 11, 2019)

**Email:** dom@spotify.com

# Oregon Student Privacy Alliance Agreement V1 with Exhibit - EXTERNAL

Final Audit Report 2019-05-11

| | |
|---|---|
| Created: | 2019-05-08 |
| By: | Meredith Allen (meredithp@spotify.com) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAb7iaoIqWZtAhXUGPlq7KG2uXgeHR_YbZ |

## "Oregon Student Privacy Alliance Agreement V1 with Exhibit - EXTERNAL" History

Document created by Meredith Allen (meredithp@spotify.com)
2019-05-08 - 6:29:41 PM GMT- IP address: 89.107.56.68

Document emailed to Dominik Sanya (dom@spotify.com) for signature
2019-05-08 - 6:30:07 PM GMT

Document viewed by Dominik Sanya (dom@spotify.com)
2019-05-11 - 5:24:38 PM GMT- IP address: 66.102.8.141

Document e-signed by Dominik Sanya (dom@spotify.com)
Signature Date: 2019-05-11 - 5:26:36 PM GMT - Time Source: server- IP address: 98.116.175.85

Signed document emailed to Dominik Sanya (dom@spotify.com), Meredith Allen (meredithp@spotify.com), pere@spotify.com, and Matteo Ottaviani (matteoo@spotify.com)
2019-05-11 - 5:26:36 PM GMT

Adobe Sign