

# **Standard Student Data Privacy Agreement**

**IL-NDPA v1.0a**

School District or LEA

Valley View School District 365U

**and**

Provider

Spotify USA Inc.

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between Valley View School District 365U located at 801 West Normantown Road Romeoville, IL 60446 (the “**Local Education Agency**” or “**LEA**”) and Spotify USA Inc., located at 150 Greenwich Street, 62<sup>nd</sup> Floor, New York, NY 10007, USA (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”. (Optional)**
  - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Astrid Welch Title: Executive Director of Technology

Address: 755 Dalhart Ave., Romeoville, IL 60446

Phone: 815-886-2700 Email: welchat@vvsd.org

The designated representative for the Provider for this DPA is:

Name: Chad Reisfelt Title: Sales Manager

Address: 150 Greenwich Street, 62<sup>nd</sup> Floor, New York, NY 10007, USA

Phone: (510) 292-9232 Email: orders@soundtrap.com

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**LEA:** Valley View School District 365U

By:  Date: 4/20/2022

Printed Name: Astrid Welch Title/Position: Executive Director of Technology

**Provider:**

By:  Date: July 14, 2022

Printed Name: Chad Reisfelt Title/Position: Sales Manager

## **STANDARD CLAUSES**

Version 1.0

### **ARTICLE I: PURPOSE AND SCOPE**

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- 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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

- 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 DPA 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 LEA as it pertains to the use of Student Data, notwithstanding the above.
- Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data 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 reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) 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.
- Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### **ARTICLE III: DUTIES OF LEA**

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data 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 Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student 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.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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 the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or 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 LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - 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; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements 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.
  - (3) 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 summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) 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 TERMS**

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** 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. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data 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, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.



5. **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.
6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, 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.
9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## **EXHIBIT "A"**

### **DESCRIPTION OF SERVICES**

Soundtrap for Education is an online audio recording studio, where teachers and students can collaborate in a safe classroom using any device. Soundtrap for Education allows you to create a secure learning environment designed to ensure the safety of your students.

Soundtrap for Education has various loops, sound effects and virtual instruments, live video collaboration and feedback features. You can also connect keyboards, guitars, microphones and any other type of ancillary music equipment. Your students can create music in any genre, record a class choir ensemble, or produce podcasts.

Soundtrap for Education is currently used in over 200 countries from elementary school to university.

**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.	<input checked="" type="checkbox"/>	
	Other application technology metadata-Please specify:	<input checked="" type="checkbox"/>	
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>	
Assessment	Standardized test scores	<input type="checkbox"/>	
	Observation data	<input type="checkbox"/>	
	Other assessment data-Please specify:	<input type="checkbox"/>	
Attendance	Student school (daily) attendance data	<input type="checkbox"/>	
	Student class attendance data	<input type="checkbox"/>	
Communications	Online communications captured (emails, blog entries)	<input checked="" type="checkbox"/>	Internal Chat only
Conduct	Conduct or behavioral data	<input type="checkbox"/>	
Demographics	Date of Birth	<input type="checkbox"/>	
	Place of Birth	<input type="checkbox"/>	
	Gender	<input type="checkbox"/>	
	Ethnicity or race	<input type="checkbox"/>	
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>	
	Other demographic information-Please specify:	<input type="checkbox"/>	
Enrollment	Student school enrollment	<input type="checkbox"/>	
	Student grade level	<input type="checkbox"/>	
	Homeroom	<input type="checkbox"/>	
	Guidance counselor	<input type="checkbox"/>	
	Specific curriculum programs	<input type="checkbox"/>	
	Year of graduation	<input type="checkbox"/>	
	Other enrollment information-Please specify:	<input type="checkbox"/>	
Parent/Guardian Contact Information	Address	<input type="checkbox"/>	
	Email	<input type="checkbox"/>	

Category of Data	Elements	Check if Used by Your System		
	Phone			
Parent/Guardian ID	Parent ID number (created to link parents to students)			
Parent/Guardian Name	First and/or Last			
Schedule	Student scheduled courses			
	Teacher names			
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		X	
	Phone			
Student Identifiers	Local (School district) ID number			
	State ID number			
	Provider/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.		X	
	Other student work data -Please specify:			
Transcript	Student course grades			
	Student course data			

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:	<input type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

## EXHIBIT "C" DEFINITIONS

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Student Generated Content:** The term "Student-Generated Content" means materials or content created by a student in the services 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.

**School Official:** For the purposes of this DPA 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; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

**Subprocessor:** For the purposes of this DPA, 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 service, and who has access to Student Data.

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

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**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 Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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**

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:

[ ]

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. Schedule 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**

Provider offers the same privacy protections found in this DPA between it and Valley View School District 365U ("Originating LEA") which is dated July 13, 2022, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("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 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. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: orders@soundtrap.com.

**PROVIDER:**

BY: Chad Reisfelt Date: July 14, 2022

Printed Name: Chad Reisfelt Title/Position: Sales Manager

**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 for the term of the DPA between Valley View School District 365U the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA:**

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: Bryan Snyder Title/Position: CIO

SCHOOL DISTRICT NAME: Cicero School District 99

**DESIGNATED REPRESENTATIVE OF LEA:**

Name: Bryan Snyder

Title: CIO

Address: 5110 West 24th Street, Cicero, IL 60804

Telephone Number: 708-863-8626

Email: bsnyder@cicd99.edu

**EXHIBIT "F"**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
X	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
X	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
X	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G" - Supplemental SDPC (Student Data Privacy Consortium) State Terms for Illinois**

Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit G**, Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between

Valley View School District 365U (the "Local Education Agency" or "LEA") and

Spotify USA Inc. (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C**, Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or

copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

8. **Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this Exhibit G, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

- a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
- b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

10. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

- a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
- b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

- d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

**11. Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

**12. Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this Exhibit G.

**13. Subcontractors.** By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

**14. DPA Term.**

- a. **Original DPA.** Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."
- b. **General Offer DPA.** The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: "The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."

15. **Termination.** Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate."
16. **Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
17. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
18. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
19. **Data Storage.** Provider shall store all Student Data shared under the DPA within the United States.
20. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

## EXHIBIT "H"

### **Additional Terms or Modifications**

Version 1

LEA and Provider agree to the following additional terms and modifications:

Standard Clauses Article II Section 3 is hereby amended as follows:

**3. Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student. For clarity, the student must be at the age of consent for data processing in their jurisdiction in order to request a transfer to a non-school account. All students under the age of consent for data processing in their jurisdiction may only request transfer of their Student-Generated Content to another school account.

Standard Clauses Article IV Section 6 is hereby amended as follows:

**6. Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after a reasonable amount of time. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as Exhibit "D". If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D." Notwithstanding the foregoing, Provider shall not be required to dispose or return any computer records or files containing Student Data that have been created pursuant to its standard archiving or backup procedures, or contained in any archived electronic communications (e.g. emails). Provider may also retain a copy of Student Data if required by applicable law, rule or regulation. The confidentiality obligations contained in this Agreement shall apply to the archived and legally required copies so long as they exist.

Standard Clauses Article V Section 2 is hereby amended as follows:

**2. Audits.** To the extent required by applicable law, no more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least twenty (20) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. Additionally, the Provider will cooperate reasonably with any local, state, or federal agency with oversight authority or 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 LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

Standard Clauses Article V Section 3 is hereby amended as follows:

**3. Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification while in its possession. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

The following sections in Exhibit G are hereby amended as follows:

Section 1. Compliance with Illinois Privacy Laws. In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance which are applicable to Provider and which may include but are not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

Section 3. School Official Designation. Pursuant to Article I, Paragraph 1 of the DPA, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

Section 4. Limitations on Re-Disclosure. The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, MHDDCA, the Service Agreement, or the DPA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA except as permitted or required by law. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA promptly in advance of the court ordered disclosure and, upon written request, provide the LEA with a copy of the court order requiring such disclosure.

Section 6. Parent Right to Access and Challenge Student Data. The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any written request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, promptly after the date of the request. In the event that a parent contacts the Provider



directly to inspect and/or copy Student Data, unless parents are afforded such rights by law or order the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

Section 7. Corrections to Factual Inaccuracies. In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider in writing of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

Section 8. Security Standards. The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from actual unauthorized access, destruction, use, modification, or disclosure, including but not limited to the actual unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA including this Exhibit G, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

Section 9. Security Breach Notification. In addition to the information enumerated in Article V, Section 4(1) of the DPA, any Security Breach notification provided by the Provider to the LEA shall include:

- a. A list of the students whose Student Data was compromised in or is reasonably believed to have been compromised in the Security Breach, if known; and
- b. The contact information of the Provider whom parents may contact to inquire about the breach.

Section 10. Reimbursement of Expenses Associated with Security Breach. In the event of a Security Breach that is attributable solely to the Provider, Provider will cover 75-100% of the actual costs and expenses incurred by the LEA for any legally required notification of authorized release of personal data to a parent or eligible student up to an aggregate amount of \$500.

Section 11. Transfer or Deletion of Student Data. The Provider regularly scans for idle accounts and those that have been idle for more than one year will be reviewed to determine whether the Student Data within those accounts that the Provider has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. As a result of this review, if any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will delete Student Data in readable form in accordance with the Service Agreement and this DPA. Upon termination of the Service Agreement between the Provider and LEA, Provider shall delete or return Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate applicable State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the

written request. Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

Section 13. Subcontractors. The Provider's list of any subcontractors to whom Student Data may be disclosed is available at [www.soundtrap.com/legal/subcontractors](http://www.soundtrap.com/legal/subcontractors). This list shall, at a minimum, be updated regularly.

Section 18. Student and Parent Access. To the extent required by law, access by students or parents/guardians to the Provider's programs or services governed by the Service Agreement or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

Section 19. Data Storage. Provider shall store all Student Data shared under the DPA within the United States, Europe and Asia.

## **Soundtrap for Education Incident Response Plan**

At Soundtrap for Education (“**Soundtrap**”), we value the trust of the schools and school districts that have chosen our services and work hard to meet or exceed legal compliance requirements. Soundtrap follows Spotify’s incident response procedures and has created this incident response plan summary to provide schools and school districts an outline of our incident response and notification procedures.

### **1. Incident Response Plan**

**1.1. Written Plan.** Soundtrap follows Spotify’s formal written incident response plan (“IRP”). The IRP describes the main processes and procedures that all Spotify companies should follow when assessing and responding to potential Information security incidents, and when remediating and resolving security incidents, including roles and responsibilities of the teams and personnel involved. It also outlines the actions that should be taken to prevent security incidents from happening, and - if they do happen - to prevent them from recurring.

### **2. Incident Response Organization**

**2.1.** There are many departments, functions and groups within Spotify that are involved in the work related to both detecting and responding to a security incident but the larger part of the work involved with preparing our response capabilities as well as active involvement in incident containment, is performed by the Legal and Security groups, lead by the Incident Manager, and supported by the Security Incident Response Team.

**2.1.1. Legal.** Among other responsibilities, Legal is the group that directs investigations into and provides legal advice regarding security incidents.

**2.1.2. Security.** Security is the group that has the overall responsibility for responding and containing security incidents, including providing a pool of Incident Managers, making sure process documentation is up to date, and that relevant tools, and resources are readily available when responding and investigating Incidents.

**2.1.2.1. Incident Manager.** All incidents need to have an assigned Incident Manager, who is responsible for leading the operational response to a particular security incident.

**2.1.2.2. Security Incident Response Team (“Security IRT”).** This is the team made up of Security individuals that is tasked with providing the necessary aid and support needed to respond to security incidents in an efficient and effective manner.

**2.2. Incident Task Force.** The task force is a group consisting of relevant stakeholders and key players required to holistically respond to and contain an Incident. Representatives will be selected by the Incident Manager based on the severity level and the facts of the security incident. Every security incident will have an incident task force.

**2.3. Incident Response Team Leads (“IRT Leads”).** The IRT Leads consist of Spotify personnel advising and deciding on high-level decisions to Security IRT and the Incident Task Force during a high severity incident. The IRT Leads are the Head of Security, the Spotify Data Protection Officer (a member of the Legal team who has overall responsibility for privacy and data protection), and a representative from the Spotify Litigation Legal team.

**2.4. Stakeholders.**

**2.4.1. Selected stakeholders.** These are groups who have a regular need to be notified about ongoing security incidents in accordance with the appropriate incident severity levels.

**2.4.2. General stakeholders.** These are groups who support the Incident Response Organization and, depending on the nature and type of the Incident, may be included as members of the ITF.

**2.5. Incident Response Process.**

Spotify’s response to an Information Security Incidents consists of three phases, as follows:

**2.5.1. Incident Reporting.** The incident is reported and relevant information is collected.

**2.5.2. Incident Intake.** The incident is triaged and severity level is assigned. Depending on severity and exposed data type IRT Leads will be engaged.

**2.5.3. Incident Handling.** The Incident Manager will lead the incident investigation. Containment actions will be identified and assigned.

### **3. School/School District Notification Procedures**

**3.1. Breach Notification.** To the extent a security incident involves student data, Soundtrap will notify impacted schools or school districts promptly and without unreasonable delay, and in line with what is contractually agreed to with the school or school district, after discovering and confirming unauthorized acquisition, access, use, or disclosure of student data by an unauthorized person.

- 3.1.1. The security breach notification will be written in plain language and titled “Notice of Data Breach” and will present strictly relevant information known at the time of the notification, using headlines such as:
  - “What happened”,
  - “What information was involved”,
  - “What Soundtrap is doing”,
  - “What the school/school district can do”, and
  - “For more information”.
- 3.1.2. Information provided in the breach notification will include at least those contractually agreed to with the school or school district.
- 3.1.3. If additional relevant information comes to light after Soundtrap has notified the appropriate school or school district of a breach, supplemental information may be provided.

**3.2. Student Notification.** Schools and school districts are responsible for notifying affected students and/or their parents, unless otherwise required by law. Soundtrap will use reasonable efforts to assist in such notification efforts.

## **Soundtrap for Education Data Security and Privacy Plan**

At Soundtrap for Education (“**Soundtrap**”), we value the trust of the schools and school districts that have chosen our services and work hard to meet or exceed legal compliance requirements. Soundtrap has created its privacy and security program centered on the principles of Appropriate Data Ownership, Limited Use, Restricted Sharing, School and Parent Control, and Meaningful Notice and Consent. The purpose of this Data Security and Privacy Plan (the “**Plan**”) is to provide schools and school districts a summary outline of how we implement applicable state, federal, and local data security and privacy requirements over the life of the contract with an education agency.

### **1. Compliance**

**1.1. Compliance with Applicable Law.** Soundtrap is designed to comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including GDPR, FERPA, COPPA, and the student privacy laws of the states in which it has contracts.

**1.2. Compliance with Student Privacy Pledge.** Soundtrap is a signatory of and complies with the [Student Privacy Pledge](#).

### **2. Appropriate Data Collection and Ownership**

**2.1. Data Ownership.** Student data provided to Soundtrap in connection with providing services to educational institutions remains the property of the applicable school or school district.

**2.2. Data Collection.** Soundtrap does not collect, maintain, use or share student data beyond the data adequate, relevant, and necessary for the purposes of providing its services, or as authorized by the parent or adult student.

### **3. Limited Use**

Soundtrap uses the student data collected through or processed by our service for limited purposes.

**3.1. Providing the Services.** We use student data only to provide these educational services and to maintain, develop, support, improve, or diagnose the Soundtrap services. We may also use data for adaptive or customized learning for students, such as responding to a student’s unique needs.

**3.2. De-Identified and Aggregate Data.** Soundtrap may use de-identified or aggregate data under limited circumstances, such as to develop or improve our services.

- 3.3. No targeted advertising.** Soundtrap does not use or sell student data for advertising purposes, including to market or advertise to students or families or to inform, influence, or enable marketing, advertising, or other commercial efforts by Soundtrap, Spotify, or any third party.
- 3.4. No profiling.** Soundtrap does not use student data to build profiles of students except to provide the services.

#### 4. Data Sharing

- 4.1. Limited Disclosures.** Soundtrap does not share student data outside of the school that we are serving, other than with subcontractors acting on our behalf, authentication partners, that enable students to use our services, or as necessary to respond to legal processes.
- 4.2. No Sale.** Soundtrap does not sell or rent student data under any circumstances. Any merger, acquisition, or sale of Soundtrap's assets is not considered a "sale" of personal data.
- 4.3. Successor Entities.** In the event of merger or acquisition, we will make efforts to ensure the successor entity honors the privacy commitments made in this Plan and our contracts, and/or we will notify you of such a sale and provide you an opportunity to opt out by deleting your account before the data transfer occurs.

#### 5. Access and Deletion

- 5.1. Data Access.** Soundtrap permits parents and adult students to review the data held about them or their student, where required by and consistent with applicable law.
- 5.2. Accuracy.** Parents, students, teachers, and principals can challenge the accuracy of data held by Soundtrap. Soundtrap will evaluate all accuracy claims and will update inaccurate data where applicable.
- 5.3. Data Deletion Upon Request.** Soundtrap permits educational institutions, parents, and adult students to request deletion of student data and will delete such data upon request as soon as practicable. Soundtrap may not delete data if the request was made by an educational institution and Soundtrap has obtained the consent of the parent or adult student to retain the data. Educational institutions, parents, and adult students who wish to delete data held about them or their students can contact Soundtrap in writing to make a deletion request.
- 5.4. Data Deletion or Transfer When Data is No Longer Needed.** Soundtrap deletes or disposes of student data when it is no longer needed for the purpose for which it was obtained. Disposition may be accomplished by modifying or anonymizing the personal information in the student data records to make it unreadable or indecipherable.
  - 5.4.1.** Student data in all active accounts and users will not be deleted unless sections 5.3 or 5.5 applies.

- 5.4.2. Soundtrap deletes, disposes of student data within a reasonable time frame when it is no longer required or needed.
- 5.4.3. Soundtrap regularly scans for idle users and/or accounts and those that have been idle for more than one year will be deleted along with the student data contained in the account.

**5.5. Deletion and Return Upon Contract Termination.** Soundtrap deletes or returns student data when our contract with the educational institution ends, subject to a 6 month grace period for trial accounts and 90 day grace period for purchased accounts. The grace periods are built in for purposes of allowing schools to renew their subscription, account for summer and winter breaks, save user generated content, etc. Upon written request by the educational institution, Soundtrap will certify the destruction of student data to the educational institution. Soundtrap will retain information only where necessary to comply with a legal obligation. Upon a written request of the school, parent or adult student, Soundtrap will migrate content the applicable student has created on Soundtrap to another school's account.

## 6. Notice and Consent

- 6.1. **Privacy Policy.** Soundtrap maintains a privacy policy that accurately describes the information that Soundtrap collects from schools and students, how the information is collected by Soundtrap, the learning purpose for which it is collected, how the information is used by Soundtrap, and with whom Soundtrap shares the information. We will not make material changes to our privacy policy without notice or choice.
- 6.2. **Consent Collected by Schools.** Soundtrap mainly engages with students and parents through schools and school districts. When we do this, we require schools to gather parental or, depending on the student's age, student consent.

## 7. Security Standards

- 7.1. Soundtrap maintains a comprehensive information security program that implements appropriate administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of student data in its custody. The high level description of safeguards in this section are just some of the ways we protect student data and honor our contractual and legal commitments.
- 7.2. **Administrative Safeguards**
  - 7.2.1. **Written Plan.** Soundtrap maintains a written information security program, including an incident response plan, aligned to the NIST Cybersecurity Framework.



- 7.2.2. **Responsible Official.** Soundtrap has designated a responsible official to manage and ensure compliance with the information security program.
- 7.2.3. **Use of Subcontractors.** When Soundtrap discloses student data to subcontractors, Soundtrap requires that its subcontractors only use the data to provide the services and imposes data protection obligations no less protective than those required under state and federal law and applicable contracts.
- 7.2.4. **Training.** Soundtrap employees are periodically trained on maintaining the confidentiality of student data, including as required by applicable laws and regulations. Soundtrap employees receive this training prior to obtaining access to student data and receive general privacy and security training during employee onboarding. Additional role-specific training is required for certain employees who have access to student data, such as technical personnel (e.g., engineers) and customer support personnel. Spotify also requires subcontractors to impose similar training requirements for its employees who access personal data.
- 7.2.5. **Risk Assessment.** Soundtrap conducts periodic physical and digital risk assessments to identify data security risks and vulnerabilities, and remediates any identified security and privacy vulnerabilities in a timely manner.
- 7.2.6. **Breach Response.** Soundtrap has an incident response plan as well as appropriate procedures to detect, contain, and respond to security incidents.
- 7.2.7. **Breach Notification.** Soundtrap will notify impacted schools or school districts promptly and without unreasonable delay, confirming unauthorized acquisition, access, use, or disclosure of student data by an unauthorized person. Educational institutions are responsible for notifying affected students or their parents.
- 7.2.8. **Data Backup and Recovery.** Soundtrap ensures that data stored locally and with third parties is appropriately backed up and can be promptly recovered in the event of a security incident or other incident that affects access to or the integrity or availability of data.

### 7.3. Technical Safeguards

- 7.3.1. **Secure Configuration.** Soundtrap maintains all student data in a secure digital environment and hosts data in an environment using a firewall updated according to industry standards. Soundtrap actively manages the configuration of both network and end user devices to ensure the security of student data. Data is currently stored in the U.S. and EU. As we expand our client base and improve our services, we may also store data in Asia.
- 7.3.2. **Data Protection:** Soundtrap takes industry standard measures to prevent data exfiltration and ensure the security of its systems and data.

- 7.3.3. Encryption of Student Data.** Soundtrap encrypts student data while in motion and at rest, using industry appropriate technology.
- 7.3.4. Access Controls.** Soundtrap limits internal access to student data to only those employees or subcontractors that need access in order to provide the services.
- 7.3.5. Intrusion Prevention and Detection.** Soundtrap deploys appropriate software and services to prevent and detect intrusions into its network.

#### **7.4. Physical Safeguards**

- 7.4.1. Facility Access:** Soundtrap has appropriate physical security measures in place to limit access to its facilities.
- 7.4.2. Physical Access to Network.** Soundtrap regularly monitors physical access to its network and assets to detect potential threats.

This Plan is periodically reviewed and updated to ensure that we comply with changes to applicable international, federal, state, and local data security and privacy. All employees of Soundtrap and third parties engaged by, or on behalf of Soundtrap are responsible for information security as part of their job responsibilities, hence all are expected to comply with Soundtrap overarching policies, guidelines and instructions.