

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Spotify USA Inc. ("Service Provider") on 12/16/2020 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.
Agree: Yes No
5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
Agree: Yes No
6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
Agree: Yes No
7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
Agree: Yes No
8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
Agree: Yes No
9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.
Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Michael Bell

Print Name

Michael Bell

Dec 17, 2020

Signature, Date

Laura Assem

Print Name (Roseville City School District)

Laura Assem

Dec 17, 2020

Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section 1.7: Internal Security

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section II.2: Exporting of Student-Created Content

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

EXHIBITS

Section II.5: Securing Student Data

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section II.6: Disclosure Notification

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

Section III.5: How Student Data is Protected:

Please see the following resources:

External Data Security and Privacy Plan (attached)
External Summary Incident Response Plan (attached)
Privacy Policy: <https://www.soundtrap.com/legal/privacy/edu>
Trust Center: <https://www.soundtrap.com/legal/trust-center>

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 principles 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. **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.
- 7.2.5. **Breach Response.** Soundtrap has an incident response plan as well as appropriate procedures to detect, contain, and respond to security incidents.
- 7.2.6. **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.
- 7.2.7. **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.
- 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.









rcsd_student_data_privacy_07-2019

Final Audit Report

2020-12-17

| | |
|-----------------|--|
| Created: | 2020-12-17 |
| By: | Chad Reisfelt (chadr@spotify.com) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAA-DKkBCpBbgVbuEopm6mo592bVq1sFtda |

"rcsd_student_data_privacy_07-2019" History

-  Document created by Chad Reisfelt (chadr@spotify.com)
2020-12-17 - 5:52:57 PM GMT- IP address: 73.158.137.126
-  Document emailed to Michael Bell (mbell@spotify.com) for signature
2020-12-17 - 5:54:35 PM GMT
-  Email viewed by Michael Bell (mbell@spotify.com)
2020-12-17 - 9:54:36 PM GMT- IP address: 66.102.7.179
-  Document e-signed by Michael Bell (mbell@spotify.com)
Signature Date: 2020-12-17 - 9:54:51 PM GMT - Time Source: server- IP address: 108.233.250.251
-  Document emailed to Laura Assem (lassem@rcsdk8.org) for signature
2020-12-17 - 9:54:53 PM GMT
-  Email viewed by Laura Assem (lassem@rcsdk8.org)
2020-12-17 - 11:31:26 PM GMT- IP address: 66.102.7.177
-  Document e-signed by Laura Assem (lassem@rcsdk8.org)
Signature Date: 2020-12-17 - 11:32:47 PM GMT - Time Source: server- IP address: 162.205.221.83
-  Agreement completed.
2020-12-17 - 11:32:47 PM GMT