RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and OverDrive, Inc. ("Service Provider") on _____ ("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 ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

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 ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

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 ( )

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

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.

Erica Lazzaro
Print Name

DocuSigned by:
Erica Lazzaro
5DF276BA527A480...
Signature, Date
1/14/2022

Laura Assem, 2/1/2022
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section 1.6: External Security

OverDrive utilizes firewalls, NSGs, vulnerability scans, and web proxies. A third-party performs an annual penetration test of OverDrive's internal and external systems.

Section 1.7: Internal Security

Student data (e.g., student ID numbers for authentication prior permitting the checkout of digital content (ebooks and audiobooks)), will be shared by LEA with OverDrive using LEA's District's preferred method of Federated, LDAP, SSO, or other similar authentication protocol. OverDrive utilizes RBAC so that student data is only accessible to employees who need access in order to perform their job functions. Backups are performed regularly and backup data is stored at a secure off-site location. A third-party performs an annual penetration test of OverDrive's internal and external systems.

Section II.2: Exporting of Student-Created Content

Student-created content is not a supported function of Sora.

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

Parents, legal guardians, and students can submit a request to review and correct their PII by emailing privacy@overdrive.com or by visiting OverDrive's Data Request Center located at https://company.cdn.overdrive.com/policies/data-request.htm. As set forth in this Agreement, LEA owns all student data, so any such request received by OverDrive would be forwarded to LEA.

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

OverDrive utilizes RBAC so that student data is only accessible to employees who need access in order to perform their job functions. OverDrive utilizes physical and technical access controls to protect data. Physical access controls include ID badges, cameras, and access reviews. Technical controls include password protection, network segmentation, and multifactor authentication.

Section II.6: Disclosure Notification

In the event that applicable PII is accessed or obtained by an unauthorized individual, OverDrive will notify the LEA's designated contact within forty-eight hours following discovery of the incident. The notification will be in writing and will include:

- The school which was the subject of the breach.
- The type of information that was reasonably believed to be subject of the breach.
- If possible, the estimated date of the breach or date range of the breach.
- Whether the notification of breach was delayed as a result of a law enforcement investigation.
- A general description of the breach incident.

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

OverDrive complies with FERPA by not selling or sharing student data, and by giving parents, legal guardians, and students and avenue to review and correct their information.

Section III.5: How Student Data is Protected:

Please see our responses above.