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 for Data Privacy and Protection

This agreement is entered into between **Roseville City School District** ("LEA") and Seesaw Learning, Inc. ("Service Provider") December 13, 20 ("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 X 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 X 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 X No _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

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 and Technology Services management.
   Agree: Yes X 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 X 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 X 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 X 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 X No _____

9. **TERMINATION:** Upon termination of this agreement as provided herein, vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify destruction of LEA data within 90 days of contract termination.
   Agree: Yes X No _____

10. **NOTICE OF BREACH:** Vendor must notify Roseville City School District's Superintendent and Director of Technology of any breach to the security of the system or breach in the security of the data, in the most expedient time possible and without unreasonable delay (Cal. Civ. Code §1798.29).
    Agree: Yes X No _____

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 X 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 X No _____

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract
   Agree: Yes X 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 X No _____

5. Vendor will attach to this document evidence how student data is kept secure and confidential
   Agree: Yes X 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 X 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 X No _____

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA
   Agree: Yes X 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 X No _____

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 X No _____
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract
   Agree: Yes X No _____
3. Vendors cannot sell student information
   Agree: Yes X No _____
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons
   Agree: Yes X No _____
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices
   Agree: Yes X No _____
6. Vendors must delete district-controlled student information when requested by the school district
   Agree: Yes X No _____
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
   Agree: Yes X No _____

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

_____ 12/13/2018

Roseville City School District — Date

_____ 12/13/2018

Nicole Bowler, K-12 Partnerships Team — Date

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

Seesaw routinely conducts 3rd party security audits to verify the security and integrity of

Section I.7 Internal Security:

We have adopted an internal data access policy that restricts access to personally identif

Section II.2 Exporting of student created content:

https://help.seesaw.me/hc/en-us/articles/208754866-

Section II.4 Review and correcting personally identifiable information:

If you are a parent or teacher, you can update the information associated with your Sees

Section II.5 Securing student data:

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Section II.6 Disclosure notification:

In the event that Student Data is accessed or obtained by an unauthorized individual, Se

Section II.8 FERPA compliance:

Data collected by Seesaw may include personally identifiable information from education

Section III.5 How student data is protected:

https://help.seesaw.me/hc/en-us/articles/203258429-How-does-Seesaw-help-keep-stude

Section I.6 External Security

- Seesaw uses SSL security at the network level to ensure all account information and journal content is transmitted securely.
- Journal Content (e.g., the photos, video, audio, and other content you add to your Seesaw journal) is encrypted at rest.
- All passwords are salted and hashed using PBKDF2.
- Seesaw routinely conducts 3rd party security audits to verify the security and integrity of our systems and internal controls.
- Account information is stored in highly secure, access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers.
- All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.

Section I.7 Internal Security:

- We have adopted an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support).
- All employees undergo a background check before beginning employment at Seesaw, sign a nondisclosure agreement, and immediately lose access to all internal systems and data when terminated. No customer information is stored on individual employee computers.
- We routinely monitor our systems for security breaches and attempts at inappropriate access.

Section II.2 Exporting of student created content:

https://help.seesaw.me/hc/en-us/articles/208754866-

Section II.4 Review and correcting personally identifiable information:

- If you are a parent or teacher, you can update the information associated with your Seesaw account directly by logging into your Seesaw account and viewing the Account Settings tab on your profile.
- If you are a parent and want to correct, edit, download, or update information about a student, please work directly with your teacher or school, or you can contact us at help@seesaw.me.

Section II.5 Securing student data:

Seesaw takes protecting your security and privacy seriously and we've put a number of measures in place to protect the integrity of your information, including:

- Use of highly secure, access-controlled data centers
- Routine third-party security audits
- Data encryption in transit
- Encryption of Journal Content at rest

For more information, please read https://help.seesaw.me/hc/en-us/articles/203258429.

Section II.6 Disclosure notification:

In the event that Student Data is accessed or obtained by an unauthorized individual, Seesaw shall provide notification to the school or district within a reasonable amount of time after the incident is discovered, and not exceeding forty eight (48) hours. We will follow the school or district's lead in deciding how to notify teachers, parents, and students.

Seesaw shall follow the following process:

1. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
2. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
    a. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    b. 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.
    c. 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.
    d. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
3. Provider agrees to adhere to all requirements in applicable state and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

Section II.8 FERPA compliance:

Seesaw is compliant with FERPA.

Data collected by Seesaw may include personally identifiable information from education records that are subject to the Family Educational Rights and Privacy Act, “FERPA”, ("FERPA Records"). To the extent that Student Data includes FERPA Records, you designate Seesaw as a "School Official" (as that term is used in FERPA and its implementing regulations) under the direct control of the school with regard to the use and maintenance of the FERPA Records and Seesaw agrees to comply with FERPA.

Section III.5 How student data is protected:

Seesaw takes protecting your security and privacy seriously and we've put a number of measures in place to protect the integrity of your information, including:

- Use of highly secure, access-controlled data centers
- Routine third-party security audits
- Data encryption in transit
- Encryption of Journal Content at rest

For more information, please read https://help.seesaw.me/hc/en-us/articles/203258429.