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 SMARTeacher Inc ("Service Provider") June 20, 2019 ("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 Y 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 Y 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 Y 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ 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 Y_____ No _____

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

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

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

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

10/3/2019

Roseville City School District — Date

DocuSigned by:
Wesley Pritchard
E28BB740D16241B...

6/20/2019

SMARTeacher Inc — 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:

Section I.7 Internal Security:

Section II.2 Exporting of student created content:

Section II.4 Review and correcting personally identifiable information:

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:

Section II.8 FERPA compliance:

Section III.5 How student data is protected:

Rosehill Data Privacy

Section 1: General (All data)

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

Prodigy uses AWS cloud services to host the infrastructure and AWS is SOC 1/2/3 complaint. Please find attached AWS Security, Confidentiality, and Integrity report.

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

The uploaded data from the district is stored in the databases hosted by AWS cloud services. Prodigy protects personal information by only allowing a limited subset of employees who have access to production data. In terms of infrastructure, Prodigy segments network topology to restrict access to the data storage layer to a limited subset of employees. Backups are performed using AWS RDS' automatic backup service. Access is restricted to the operational team and select members of the data team. Backups are maintained for a rolling seven to fourteen day period and upon expiry are deleted. Data is never printed by the operational teams.

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

We can use SFTP to transfer all the district data to Prodigy. We are in the process of developing the systems for third-party logins like Clever, ClassLink.

Section II: AB1584 Compliance (Student information only)

2. Vendor must attach to this document a description of how student created content can be exported and/or transferred to a personal account

The content generated by the student stays in the game. It can't be exported to a personal account.

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information

Account Settings page allows our users to review/correct the personal identifiable information (name. School, password, etc.).

5. Vendor will attach to this document evidence how student data is kept secure and confidential

- Data stores are segregated into private subnets which have restricted network access.
- Disk storage and transport is encrypted using industry standard encryption.
- Backup access is restricted to select team members and audited
- Secrets are stored encrypted, access to them is restricted and usage is by injection into applications at run time.
- All data layer access is audited via industry standard tooling.

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

In case of an incident, we would notify parents, legal guardians, via an email of any unauthorized access or disclosure to student records.

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA

Prodigy utilizes AWS to host the math platform. Linked below is the FERPA compliance from AWS.

https://aws.amazon.com/blogs/security/ferpa-compliance-in-the-aws-cloud/

9. Vendor and its agents or third parties are prohibited from using personally indentifiable information from student records to target advertising to students.

During school hours and when students play Prodigy from school, there are no advertisements to students. If students elect to play at home, there is an optional parental membership pop-ups. This membership allows Prodigy to provide the platform at zero cost to districts. In addition, there are no 3rd party ads during gameplay.