Roseville
CITY SCHOOL DISTRICT

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • 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 **Front Row Education** (“Service Provider”) **10/30/2017** (“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:

<u>Section I: General</u> (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 _______

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 _______

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 _______

<u>Section III: SB 1177 SOPIPA Compliance</u> (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.

________________________________ 10/30/2017

Roseville City School District Date

________________________________ 10/30/2017

Maggie Kenny, Account Executive | Front Row Date

Exhibits

Section I.6 External Security:

Front Row backend servers are hosted on Amazon Web Services. Only the application and API servers are accessible from the Internet at port 80 and 443. All communication between the application backend servers and the application clients is done over HTTPS. All applications are behind an Elastic / Application / Network load balancer provided by Amazon Web Services. Network isolation and firewalls are provided by Amazon Web Services Virtual Private Cloud (https://aws.amazon.com/security/) .

Additionally a bastion server to enable production VPN access for Front Row engineers is exposed on the internet on port 22 and uses Public / Private Key Infrastructure encryption.

Section I.7 Internal Security:

Access to district data is issued on a per-need basis to Front Row staff. Access is controlled at either Amazon Web Services level through Identity and Access Management module or for analytics purposes through the Periscope Data application.

District data is uploaded to the system through either the application itself, or through internal tooling run by Front Row's customer success agents or operations engineers.

All data is encrypted at rest. Backups are handled entirely by Amazon Web Services Relational Database Service (RDS) and its backups are also encrypted at rest. Production data backups are only accessible to operations engineers. Backups are kept around for 30 days after which they are deleted.

District data is not printed.

Section II.2 Exporting of student created content:

Students are unable to create content in Front Row.

Section II.4 Review and correcting personally identifiable information:

Parents, legal guardians, and students currently cannot correct their personally identifiable information, only teachers and school / district admins can correct student information.

Section II.5 Securing student data:

Student data (First name, last name, records of practice) is stored encrypted at rest in Amazon Web Services Relational Database Service and Simple Storage Service. Student data is only accessible by users of the system that have the authority to do so, such as the student herself, the student's teachers and the student's school and district administration. Student data is only ever transferred on the Internet over HTTPS. Student data is only accessible to Front Row operations engineers and analysts.

Section II.6 Disclosure notification:

In case of unauthorized disclosure of student records, the teachers and administration of the affected schools will be notified as soon as possible over email and investigation will be made into how the disclosure happened and how it will be prevented in the future.

Section II.8 FERPA compliance:

Front Row allows parents to have full visibility of their student's data. We accomplish this by allowing their child's teacher to to share their child's data with the use of a free Front Row account, created at www.frontrowed.com, and then configuring this parent account with their child school. Teachers can also print and send data reports home to parents.

Section III.5 How student data is protected:

Student data (First name, last name, records of practice) is stored encrypted at rest in Amazon Web Services Relational Database Service and Simple Storage Service. Student data is only accessible by users of the system that have the authority to do so, such as the student herself, the student's teachers and the student's school and district administration. Student data is only ever transferred on the Internet over HTTPS. Student data is only accessible to Front Row operations engineers and analysts.