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 Fuel Education LLC ("Service Provider") on 9/28/2021 ("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.

Patrick Neeman
Print Name

DocuSigned by:
Patrick Neeman
82588F0571BB456...
9/28/2021
Signature, Date

Laura Assem, Executive Director of Technology
Print Name (Roseville City School District)

9/28/2021
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

• Stride Learning Management Systems are hosted within Amazon Web Services. Stride utilizes AWS Web Application Firewall rules and WAF patterns to secure AWS hosted systems from external attack. Stride also utilizes other AWS supporting technologies such as Cloud Trails, Guard Duty, and Security Hub to support protection from and detection of external attacks.

Section 1.7: Internal Security

Only approved personnel would have access to RCSD data. We have employees with database level access to all data. Employees on the business side that are supporting the district will be granted access to district data (Client success managers, Implementation, Training and operational support staff as needed). Uploads are managed by RCSD. They would upload data directly to the system. Stride utilizes a combination of logical access controls, user activity controls, multifactor authentication, endpoint and system hardening controls, email security controls, application security controls, software development lifecycle / change management controls, and 24x7 security managed detection services to protect student data. Data access is governed by policy and data classification standard which guides role-based access based on job duty requirements. Additionally, Stride works with trusted partners and internal stakeholders to continuously strengthen data protection governance, policies, practices, and processes aligned with the relevant regulations and control frameworks such as FERPA, SOX, NIST CSF, etc. Stride leverages internal governance

Section II.2: Exporting of Student-Created Content

During the duration of our partnership teachers will have direct access to student created content that has been submitted for students assigned to their classrooms. Teachers can locate student submissions directly in the gradebook. Once identified teacher can view directly in the platform or download to be transferred to a private account. In additional district administrative staff can request documents through their client success manager or by phone 844-638-3533

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

Parents, legal guardians, or eligible pupils may review Pupil Records and correct erroneous information by the following protocol: Requestors eligible to review and correct such documents under applicable law shall submit such requests to Customer. If such data is available to Customer through its account administration on a FuelEd learning management system, Customer shall respond to the request directly. If the requested information is not available to Customer, Customer shall then forward valid requests to FuelEd. FuelEd will respond by providing the Pupil Record to Customer in a mutually agreed upon media format or make corrections to a Pupil Record, both in a commercially reasonable time.

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

FuelEd shall take actions to ensure the security and confidentiality of Pupil Records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of Pupil Records, by the following measures: Operate its systems infrastructure at the moderate level baseline as defined in the National Institute of Standards and Technology ("NIST") 800-53 Rev. 3 moderate baseline requirements, and/or in accordance with industry accepted cyber-security standards. Through the aforementioned actions and other industry accepted means, FuelEd shall ensure compliance with FERPA.

Section II.6: Disclosure Notification

In the event of an unauthorized disclosure of a Pupil Record, FuelEd shall report to an affected parent, legal guardian, or eligible pupil pursuant to the following procedure: Upon internal confirmation of an unauthorized disclosure of a Pupil Record belonging to a pupil served by Customer, FuelEd shall contact Customer with information related to the disclosure. Customer will then contact the affected parties and inform them of the unauthorized disclosure.

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

FuelEd shall take actions to ensure the security and confidentiality of Pupil Records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of Pupil Records, by the following measures: Operate its systems infrastructure at the moderate level baseline as defined in the National Institute of Standards and Technology ("NIST") 800-53 Rev. 3 moderate baseline requirements, and/or in accordance with industry accepted cyber-security standards. Through the aforementioned actions and other industry accepted means, FuelEd shall ensure compliance with FERPA.

Section III.5: How Student Data is Protected:

See above.