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, Executive 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 Codesters ("Service Provider") on 03/18/2022 ("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.

Juan Farfan (CTO)
Print Name

Juan Farfan 03/18/2022
Signature, Date

Laura Assem, 3/22/2022
Print Name (Roseville City School District)

Laura Assem
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Student data in Codesters is stored and processed through Amazon Web Services. Some of the security features enabled on AWS include:
- All connections to servers and databases pass through a virtual public cloud (VPC) with enhanced monitoring enabled on all services
- Network traffic is managed by a load balancer with an attached security group and firewall rules
- Direct server access is tightly controlled with SSH keys that are rotated on a yearly basis
- Databases are encrypted and access can only be established through servers on the same VPC

Section 1.7: Internal Security

Codesters maintains a "Student Privacy Guide" and "Information Security Policy" for internal employees with strict requirements for handling student data. A few of the relevant provisions are:
- Employee requirements for accessing student data: annual security trainings, criminal background checks, password/SSO/2FA policies, onboarding & offboarding processes, etc.
- Requirements for student data collection, transmission, storage, and disposal to secure student PII: end-to-end encryption, data disposition rules, subprocessor management
- Data access and authorization protocols in line with all applicable Federal laws, CA State laws, and the California Student Data Privacy Agreement (v2)

Section II.2: Exporting of Student-Created Content

In order to export student data to an individual account, a written request must be sent via email to your Codesters account administrator or to support@codesters.com.

Requests to export student data to an individual account are considered authorized requests and must be approved by a district administrator. The only exception is a request from an authorized user (parent, legal guardian, eligible student, or law enforcement as defined in FERPA), in which case the district administrator will be notified but does not need to approve the data transfer.

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

Personally identifiable student data can be reviewed by a student in their Codesters dashboard under "Account Settings". Depending on the rostering method of the district, a student may or may not be able to modify his or her information directly in the platform. A district administrator or teacher should have the ability to modify this information.

For parents, legal guardians, or eligible students as defined in FERPA, a request to modify PII can be made by contacting support@codesters.com. We will notify a district administrator of such a request.

EXHIBITS

Section II.5: Securing Student Data

As described in the above exhibits to Section 1.6 & Section 1.7, Codesters maintains comprehensive security controls over external & internal data access.

The policies and protocols concerning student data are governed by a "Student Privacy Guide" that all employees are required to read and receive training on. This document is reviewed annually and updated to reflect ongoing updates to laws and security agreements. Currently, the "Student Privacy Guide" is written to comply with:
- Federal Laws (FERPA, COPPA, PPRA)
- CA State Laws (AB 1584, SOPIPA)
- California Student Data Privacy Agreement (v2)

Section II.6: Disclosure Notification

The Codesters "Student Privacy Guide" includes a Data Breach Protocol with some of the following requirements to notify users of a data breach:
- The notification must go out within 48 hours of discovering the breach
- The notification must be sent to the administrators of all impacted accounts
- The notification must be titled “Notice of Data Breach”
- The notification must contain the following sections: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", "For More Information"
- The notification will not be sent directly to account members (students, parents, non-admin teachers); we expect the account administrator to notify the impacted parties as needed

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

Several of the ways that Codesters complies with FERPA are:
- Maintaining an internal "Student Privacy Guide" with policies and protocols that align to all FERPA requirements
- Requiring all employees with access to student data to sign a FERPA Non-Disclosure/Confidentiality Agreement
- Maintaining and updating subprocessor agreements to verify security compliance and to restrict access to student PII as needed

Section III.5: How Student Data is Protected:

This is described in the above exhibit to Section II.5: Securing Student Data.