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 Clever, Inc. ("Service Provider") on 11/5/19 ("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 ○

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

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 ○

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

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 ○

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

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.

Kevin Laughlin
Print Name

DocuSigned by:
Kevin Laughlin 11/5/2019
Signature, Date

Laura Assem, 11/6/2019
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

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 1.6: External Security

Service Provider stores its data in the U.S. and takes strong measures to keep data safe and secure. It maintains strict administrative, technical and physical procedures to protect information stored in its servers. It uses industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include, but are not limited to, data encryption, firewalls, and physical access controls to buildings and files. It uses bank-grade security infrastructure at the software and network level, to ensure that student records are always encrypted and transmitted securely. This includes use of TLS / SSL protocols, API call level authentication, and API bearer tokens with 200 bits of entropy. Its Transport Layer Security requires that all data transferred via its website and API use the Transport Layer Security (TLS) cryptographic protocol over a HTTPS connection. This means that unique session keys are used to encrypt and decrypt data transmissions and to validate transmission integrity. Its servers prefer perfect forward secrecy (using ECDHE) to encrypt data using 256 bit Advanced Encryption Standard (AES) – which surpasses the standard adopted by the consumer banking industry and the U.S. Government for the secure transmission of classified data.

Section 1.7: Internal Security

Service Provider limits access to PII only to those employees or trusted service providers who have a legitimate need to access such data in the performance of their duties or in connection with providing services to the District under its agreement with Service Provider. Access to information is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. Service Provider will maintain access log(s) that record all disclosures of or access to PII within its possession and will provide copies of those access log(s) to the District upon request. In addition, Service Provider provides employee training on privacy and data security laws and best practices.

Section II.2: Exporting of Student-Created Content

There is no student-created content being provided to the Service Provider by the District.

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

The Service Provider will work with the District in processing any request to review, and challenges to the accuracy of, PII in the custody of the Service Provider.

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

See Service Provider's Additional Terms of Use for Schools found at https://clever.com/trust/terms/schools, Privacy Policy found at https://clever.com/trust/privacy/policy and General Terms of Use found at https://clever.com/trust/terms for additional information about how Service Provider secures and protects student data.

Section II.6: Disclosure Notification

If there is any disclosure or access to any personally identifiable student data by an unauthorized party (a "Security Incident"), Service Provider will promptly notify the District's account owner of any affected schools via email and will use reasonable efforts to cooperate with their investigations of the incident. To the extent known, this notice will identify (i) the nature of the Security Incident, (ii) the steps Service Provider has executed to investigate the Security Incident, (iii) the type of student data affected, (iv) the cause of the Security Incident, if known, (v) the actions Service Provider has taken or will take to remediate any deleterious effects of the Security Incident, and (vi) any corrective actions Service Provider has taken or will take to prevent a future Security Incident. If the incident triggers any third party notice requirements under applicable laws, the District agree that, as the owner of the student data, it may be responsible for the timing, content, cost, and method of any required notice and compliance with those laws. However, at the request of the District and when permissible under applicable law, Service Provider agrees to bear responsibility for the timing, content and method of such required notice on behalf of the District.

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

Service Provider agrees to uphold its responsibilities under FERPA. Service Provider provides technology and services to the District under the school official exception of FERPA 34 CFR Part 99.31(a)(1).

Section III.5: How Student Data is Protected:

The PII received by Service Provider will be used only to provide technology and services to the District pursuant to its contract with the District and for no other purpose. Anyone involved in the handling of PII will treat such data as confidential and shall not redisclose such data except as necessary in order to provide services to the District. Upon the termination of the Service Provider's contract with the District, Service Provider will securely destroy or return all PII received from the District as soon as reasonably possible. Additional details about what happens to student data upon termination of the District's relationship with the Service Provider can be found in the Clever Additional Terms of Use for Schools found at https://clever.com/trust/terms/schools.