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 CloudLock LLC ("Service Provider") ________________ ("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 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 _______ No NA_______

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 _______ No NA_______

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 _______

<u>Section II: AB1584 Compliance</u> (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 _______ No NA_______

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 _______ No NA_______

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 _______

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 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

_______________________________________ 9-23-2016

Roseville City School District Date

DocuSigned by:
Rachael McCarthy
A1661EC8E36D434...

Dir. Finance 9/23/2016 | 9:07:29 AM PDT

CloudLock LLC Date

CloudLock Legal Approval

DS
LM

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:

Section II.6 Disclosure notification:

Section II.8 FERPA compliance:

Section III.5 How student data is protected:

Section I.6. External Security

In addition to the SOC3 report available here: https://www.cloudlock.com/company/trust/. CloudLock performs annual Penetration Tests. An executive summary of the report is available under NDA.

Section I.7 Internal Security

Please see the SOC3 report available here: https://www.cloudlock.com/company/trust/. If needed, CloudLock can provide the most recent SOC2 type II report under NDA as evidence of security controls.

Section II.2 Exporting of student created content

Students do not create content within the CloudLock Service so this is not applicable. Content created by students within the applicable cloud applications (e.g. Google Apps) is retained and controlled by Roseville School District.

Section II.4 Review and correcting personally identifiable information.

Please see CloudLock privacy policy at www.cloudlock.com/privacy-policy/. Also please note that CloudLock does not retain or control personal student data, with the exception of an e-mail address associated with the cloud accounts the CloudLock service is used by the school to scan. Students and/or parents/guardians should contact the Roseville School District in accordance with the Roseville School District policy as Roseville, not CloudLock, retains and controls student data.

Section II.5 Securing student data:

CloudLock does not retain student data, with the exception of an e-mail address associated with the scanned cloud application accounts. Please see external and internal security above.

Disclosure notification:

Although CloudLock does not store or control pupil records, if CloudLock confirmed an unauthorized disclosure of a pupil's records in connection with the Services, CloudLock would promptly notify Customer and, if and as required by applicable laws or if advised by legal counsel, would notify the parent, legal guardian or eligible pupil.

Section II.8 FERPA Compliance:

Customer controls the cloud accounts that the Services will have access to and will limit CloudLock's access to educational records and CDI only to the extent required for CloudLock to perform the purchased Services. CDI means data and information covered by FERPA, including paper and electronic student education record information provided or made accessible to CloudLock in connection with the performance of Services.

If access to educational records and CDI are required to perform the Services, CloudLock acknowledges that it will comply with FERPA to the extent applicable to CloudLock, including the limitations on re-disclosure of personally identifiable information from education records set forth in FERPA and the requirement that education record information may be used only for the purposes for which the disclosure was made. CloudLock shall hold any CDI provided to it in strict confidence as confidential information under the Agreement, except as permitted or required by the Agreement, as required by law, or as otherwise authorized by Customer in writing.

Section III.5. How student data is protected:

The pupil should contact Customer for the applicable process as CloudLock does not store or control pupil records or content. CloudLock stores only Customer Meta-Data as described in the Agreement. If Customer's Services include coverage for student cloud accounts, the CloudLock Meta-Data may include the student's account name (typically e-mail address) but will not include the content of files on the student's cloud account.