

Vendor Statement of Compliance for Data Privacy and Protection

This agreement is entered into between Roseville City School District (“LEA”) and CommonLit, Inc. (“Service Provider”) 6/20/2018 (“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)

- 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
- 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
- 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

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 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, 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 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 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 school 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

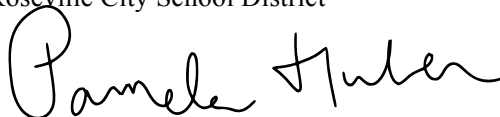
As an authorized representative of my organization, I accept the conditions listed in this document.



6/20/2018

Roseville City School District

Date



6/20/2018

CommonLit, Inc.

Date



TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • Fax (916) 771-1650

Laura Assem, Director of Technology

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:



TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • Fax (916) 771-1650

Laura Assem, Director of Technology

Section II.6 Disclosure notification:

Section II.8 FERPA compliance:

Section III.5 How student data is protected:

Section I.6

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.

We use Cloudflare, an industry-leading Web Application Firewall (WAF) that provides active attack intervention, collectively-sourced thread signatures, and pre-set rules for blocking suspicious activity.

Section 1.7

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?

On our end, members of the CommonLit team have access to this data via the Clever Portal once data is shared by the district. The District has its own agreement with Clever on how Clever protects the data when it is being uploaded from the District to Clever. Only limited personnel are provided access to the Clever Portal and all personnel have two factor authentication enabled. Backups are performed nightly, and are only available to a subset of the engineering/technical personnel, all of whom have signed privacy policy and had a background check. Expired backups are purged. As a company policy, class rosters are never downloaded or printed, so hard copies do not need to be destroyed. In the event that any personal information if ever printed, the hard copies must be shredded when no longer in use.

Our application has access scopes that prevent users from accessing data outside of their account's permissions. These scopes stretch through teacher-level, school-level, and district-level blocks. Backups are made nightly on our database provider, and are retained for one month for audit and disaster recovery scenarios. Access to backup data is restricted to a subset of our developers, each of whom can only access the data using 2-factor authentication. After the expiration date, our backups are destroyed. We do not generate hard copies of user data.

Section I.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).

We can provide an extract of all authorized data from our system using a SQL dump. Our application uses PostgreSQL, and the dump would be generated by `pg_dump` with tables truncated to only include authorized data.

Section II.2:

Vendor must attach to this document a description of how student created content can be exported and/or transferred to a personal account

Teachers can print off individual student assignment reports which contain student's assignment averages. CommonLit is updating the individual student progress page (available to students and teachers) to provide all short answer responses generated by students in 1 central location; for now, students can view individual assignments one at a time and print off (or save as a PDF) the assignment from their browser if they wish to save their short answer responses.

Section II.4

Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information

We recognize parent's rights to review their student's records and work closely with schools to ensure FERPA compliance. CommonLit is under the direct control of schools and districts and, in most relationships with schools, is acting as a school official according to FERPA.

We request that parents reach out to teachers to review or correct errors in their student's educational records stored on our site to protect against accidentally disclosing information to someone other than a true parent or guardian. When parents reach out to us directly, we instruct them to log into their child's account to review information or to reach out to the teacher. If we cannot verify a parent's identity, we contact the teacher.

Teachers have access to all of their student's records stored on the site, except for IP addresses, cookies, and passwords (though teachers can reset passwords). Therefore, teachers can share downloadable reports or screenshots from our website with parents. Teachers can correct errors at the parent's request; if there are errors the teacher cannot correct (such as out auto-generated username having incorrect spelling because a student typed their name wrong), the teacher can reach out to us and relay a parent's request, and we will amend the student's data.

Students can view and update their grade level, name, and email from their My Account page and can review their educational records from their My Progress or My Assignments pages. Teachers have some control over when students see their scores, and students can ask teachers for access to unreleased scores.

Section II.5

Vendor will attach to this document evidence how student data is kept secure and confidential

CommonLit utilizes Amazon Web Service's data centers in the continental United States to securely store assignment data, in compliance with industry standards including FERPA, COPPA, and FISMA. Data within our applications are encapsulated in PostgreSQL, encrypted at rest, and require a secure SSL connection for access with internal services to protect sensitive personally identifiable information from unauthorized access. Separate services including RedShift are utilized for large-scale warehousing and intensive data analytics.

We never use student data to advertise or market to students, in accordance with FERPA, COPPA, and SOPIPA. We notify teachers of their responsibility to obtain direct parental consent for students under the age of 13, in compliance with COPPA, before they prompt students to create student accounts. Educational records are available to parents upon request.

We also conduct third-party penetration testing and vulnerability assessments, employ HTTPS, and take countermeasures against packet sniffing, port scanning, spoofing, and DDoS attacks.

Section II.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

CommonLit's breach response plan varies based on the size of the breach and includes displaying a notice on the website, emailing affected individuals, and notifying schools and districts so they too can display a public notice or provide specific notice to parents of affected individuals. Because CommonLit does not require student emails upon sign-up (and because school servers often block our emails to students' school email accounts), CommonLit would work closely with a school or district of affected individuals to ensure that affected individuals receive proper notice within a reasonable amount of time; in the event of a large breach, CommonLit would provide notice on its website which includes directions on how to receive more specific information as an affected individual.

CommonLit has entered into agreements with California districts in the past under the following terms:

In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process: a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice. b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information: 1. The name and contact information of the reporting LEA subject to this section. ii. A list of the types of personal

information that were or are reasonably believed to have been the subject of a breach. Hi. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided. v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided. c. At LEA's discretion, the security breach notification may also include any of the following: I. Information about what the agency has done to protect individuals whose information has been breached. H. Advice on steps that the person whose information has been breached may take to protect himself or herself. d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts. e. At the request and with the assistance of the District. Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

Section II.8

Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA

CommonLit is FERPA compliant. We recognize parent's rights to review their student's records and work closely with schools to be compliant. CommonLit is under the direct control of schools and districts and, in most relationships with schools, is acting as a school official according to FERPA.

We request that parents reach out to teachers to review or correct errors in their student's educational records stored on our site to protect against accidentally disclosing information to someone other than a true parent or guardian. When parents reach out to us directly, we instruct them to log into their child's account to review information or to reach out to the teacher. If we cannot verify a parent's identity, we contact the teacher.

Teachers have access to all of their student's records stored on the site, except for IP addresses, cookies, and passwords (though teachers can reset passwords). Therefore, teachers can share downloadable reports or screenshots from our website with parents. Teachers can correct errors at the parent's request; if there are errors the teacher cannot correct (such as out auto-generated username having incorrect spelling because a student typed their name wrong), the teacher can reach out to us and relay a parent's request, and we will amend the student's data.

District administrators and principals may access student data at the school and district level using CommonLit for Leaders product with a paid subscription. These student accounts are

rostered and approved by the district administrators themselves, and we do not currently authorize access to the data to any other users without the district's explicit permission. Currently, some users access data at the district/school level using Periscope, an approved third party service.

At this time, we do not grant parents direct access to data by logging them directly into a student's account. They would have to go through the school or their child to acquire such direct access.

Our contractors are bound by the same Privacy Policy as our full-time employees. We only use third-party partners to conduct our Services if those partners are secure and have vetted Privacy Policies that ensure student and teacher data is not for sale or available for uses outside of those we authorize.

Section III.5

Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices

Section II.5 covers much of this information. In addition to the stated security practices of our website, we conduct regular staff security trainings regarding access to and security of student data. All student data available in our systems or through third party partners is protected using two factor authentication.