

Vendor Statement of Compliance for Data Privacy and Protection

This agreement is entered into between Roseville City School District (“LEA”) and
WeVideo Inc (“Service Provider”) 1/25/2018
 (“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)

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



CITY SCHOOL DISTRICT

TECHNOLOGY SERVICES

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

Laura Assem, Director of Technology

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.



Roseville City School District

1/25/2018
Date



WeVideo Inc

1/25/2018
Date

Exhibits

Section I.6 External Security:

WeVideo's cloud based infrastructure is hosted on Amazon Web Services (AWS).

~~The following link provides comprehensive information on AWS security procedures, policies, and compliance. <http://aws.amazon.com/security/>~~

Section I.7 Internal Security:

~~All transactions to access content between client and server are done using SSL. In addition file URLs are signed to ensure all access is secure and controlled. All WeVideo users have a unique username and password. The password is stored and accessed in an encrypted format. WeVideo maintains strict access control to ensure content is only accessed by users who have rights to it. All data ownership and access in the system is clearly defined and enforced for each user using their credentials.~~

Section II.2 Exporting of student created content:

~~Any content created by a student can be viewed and downloaded from the WeVideo Gallery. The downloaded file is an .mp4 video file.~~

Section II.4 Review and correcting personally identifiable information:

~~In the WeVideo Hub (after authentication) by selecting the "Manage Account" option, the user is able to view all the information collected by WeVideo. This information can also be modified on this page.~~

Section II.5 Securing student data:



CITY SCHOOL DISTRICT

TECHNOLOGY SERVICES

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

Laura Assem, Director of Technology

All transactions to access content between client and server are done using SSL.

~~In addition file URLs are signed to ensure all access is secure and controlled. All WeVideo users have a unique username and password. The password is stored and accessed in an encrypted format. WeVideo maintains strict access control to ensure content is only accessed by users who have rights to it. All data ownership and access in the system is clearly defined and enforced for each user using their credentials.~~

Section II.6 Disclosure notification:

~~If WeVideo experiences a disclosure or security breach concerning any education record covered by this Agreement, WeVideo shall immediately notify District and take immediate actions to limit and mitigate such security breach.~~

Section II.8 FERPA compliance:

~~WeVideo does not use the student information for any other purpose other than for the performance of the WeVideo software. If any person requests access to student records, WeVideo will immediately notify District of this request. It will be the District's responsibility to respond to such information requests. If WeVideo experiences a disclosure or security breach concerning any education record covered by this Agreement, WeVideo shall immediately notify District and take immediate action to limit and mitigate such security breach. Once the term of the agreement is completed, WeVideo will destroy all student information stored.~~

Section III.5 How student data is protected:

~~WeVideo's cloud based infrastructure is hosted on Amazon Web Services (AWS). The following link provides comprehensive information on AWS security procedures, policies, and compliance. <http://aws.amazon.com/security/>~~
