

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and _____ ("Service Provider") on _____ ("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.

Print Name

 03/24/2020

Signature, Date

Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Section 1.7: Internal Security

Section II.2: Exporting of Student-Created Content

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

EXHIBITS

Section II.5: Securing Student Data

Section II.6: Disclosure Notification

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

Section III.5: How Student Data is Protected:

Privacy Policy

Last Updated 2/17/2020

This Privacy Policy applies to all the Vidcode-branded websites and online applications (“Vidcode Resources”), and describes how we collect, use, store, and share information about the users of Vidcode Resources.

Privacy Laws

Vidcode makes every effort to ensure compliance with applicable privacy laws, including the Family Education Rights and Privacy Act (FERPA), Children’s Online Privacy Protection Act (COPPA), New York State Education Law 2-d, and the General Data Protection Regulation (GDPR).

Children's Privacy

Vidcode will never knowingly collect personally identifying information from children under 13, without prior verifiable parent or educator consent. In partnership with our schools, we strive to protect student’s personal information, as required by the Family Educational Rights and Privacy Act (FERPA), and to protect the personal information of students under 13 consistent with the Children’s Online Privacy Protection Act (COPPA). Any requests to review, modify, correct, or delete the personal information of a student accessing the Vidcode Resources can be made at any time by emailing info@vidcode.com (<mailto:info@vidcode.com>).

Information We Collect

Profile information

When you create an account with the Vidcode Resources, we collect personal information from you in order to authenticate login information. This personal information you provide us with may include

- username
- email address*
- self-designated role
- authentication information from third-party integrated services such as Google, Office 365, or similar single sign-on providers

* We collect email addresses for all users that create an account with us in order to uniquely identify them in our system. However, we make every effort to limit our communications to those users who identify themselves as educators or guardians and never to email students directly.

You can interact with some parts of the Vidcode Resources without creating an account or providing any personal information, and we will collect personal information from you only if you voluntarily provide it to us in connection with a registration, subscription, purchase or other use of the site.

Usage and Device Information

To provide you with a high-quality experience, certain data and non-personal identification information is automatically collected when you interact with the Vidcode Resources. This information includes things like location information, information about your browser or device, access times, pages viewed, and the referring link through which you accessed the Vidcode Resources.

Web Browser Cookies and Site Analytics

Our site uses "cookies" and similar technologies to enhance your experience. Cookies may be placed on your hard drive for record-keeping purposes, and to track information about how you are using our site. You can set your web browser to refuse cookies, or to alert you when cookies are being sent. If you do so, some parts of our site may not function properly for you.

We also work with some third-party services, such as Google Analytics, to collect and analyze information on site usage. These providers may use cookies and other technologies to collect information about your use of our site.

How We Use Your Information

We use your personal and non-personal information only for educational purposes, to provide you with the Vidcode Resources you use, and for the following:

- To respond to your comments, questions, and requests as well as to provide customer service
- To personalize and enhance your experience with our the Vidcode Resources
- To help us improve our site design, products, and services
- To analyze site trends, usage, and statistics

How We Protect Your Information

We use industry-standard Secure Sockets Layer (SSL) encryption software to help protect your information from loss, theft, misuse, unauthorized access, disclosure, alteration, and destruction.

All user data is hosted by Heroku, a Salesforce company; ObjectRocket, a Rackspace company; and Amazon Web Services. Heroku, ObjectRocket, and Amazon Web Services use SSL encryption software. These third parties are well-known, established providers, who are bound to practice adequate security measures and to use your information solely as it pertains to the provision of their services.

How We May Share Your Information

We may share your personal and other information in the following ways:

- With our third-party service providers who require access to such information to carry out work on our behalf such as web hosting, email delivery, credit card processing, and other services.
- If needed to protect the rights, property, and safety of us or any third party
- If needed to respond to the request of law enforcement in cases where we believe disclosure is required and/or in accordance with applicable law, regulation, or legal process
- We may also share aggregated or de-identified information, which cannot reasonably be used to personally identify you

Your Rights to Your Information

You can update your customer account information, manage the way that we use and do not use your information, or request the deletion of your information at any time by contacting us at info@vidcode.com (<mailto:info@vidcode.com>)

You can review your personal data we have collected at any time by contacting us at info@vidcode.com (<mailto:info@vidcode.com>).

Third Party Websites

There may be content on our site that links to the sites and services of others. We do not control these sites and services, and are not responsible for them. Those sites' terms of use and privacy policies will be applicable to your interaction with those sites and services.

Changes to this Privacy Policy

We may update this privacy policy from time to time. When we do, we revise the “updated” date at the top of this page and notify subscribers of the privacy policy update via email. If you are not a subscriber, we encourage you to review our Privacy Policy on a regular basis to note any changes made to this policy.

If you have any questions about this privacy policy, we encourage you to contact us at info@vidcode.com (<mailto:info@vidcode.com>)