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 the College Board ("Service Provider") on November 1, 2016 ("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 ___ X ____ 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 ___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 __X_____ 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 __ 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 _____

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 _ 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 __X____ No _____

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 __X_____

5. Vendor will attach to this document evidence how student data is kept secure and confidential. Agree: Yes __X_____ No _____

6. Vendor will notify LEA 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 _____

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 ___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 as indicated in the Technology Agreement, 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.

Roseville City School District

Date 11/8/2016

Date 11/7/2016

Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

Database access is only available from the application servers. The application servers themselves do not have public IP addresses and are only reachable via SSH from a single bastion server. SSH access is limited to specific whitelisted user accounts.

HTTP requests are handled via AWS Elastic Load Balancer which restricts access to the HTTP port only. No ports are open to the public at large on any production server. HTTP requests are all rewritten to use HTTPS on the back end.

The application is automatically scanned nightly by WhiteHat Security Sentinel to identify security or data vulnerabilities so that they may be immediately addressed.

Section I.7 Internal Security:

All secure data at rest is encrypted. We use https throughout our applications. District-uploaded data is handled through Clever. Transport Layer Security (TSL) protocol is employed, with authenticated API calls and Secure OAuth 2.0 API Bearer Tokens. More information here.

Access to pupil records is limited to individuals required to access this information as a core job responsibility (support and implementation managers) and is password-protected. Every authorized attempt to access student records is logged for audit purposes.

The application is automatically scanned nightly by WhiteHat Security Sentinel to identify security or data vulnerabilities so that they may be immediately addressed.

Data is not printed by internal users to avoid security issues.

Section II.2 Exporting of student created content:

If the district requests an extraction of all data from the system, data will be provided in Excel format via SFTP. Requests can be issued by contacting SpringBoard Digital Technical Support at SBTechSupport@collegeboard.org.

Section II.4 Review and correcting personally identifiable information:

N/A

Section II.5 Securing student data:

Access to pupil records is limited to individuals required to access this information as a core job responsibility (support and implementation managers) and is password-protected. Every authorized attempt to access student records is logged for audit purposes.

Laura Assem, Director of Technology

Section II.6 Disclosure notification:
Affected persons will be contacted in accordance with applicable laws

Section II.8 FERPA compliance:
We will comply with applicable provisions of FERPA regulations in accordance with our designation as a school official with legitimate educational interests by destroying applicable FERPA protected student data furnished by the LEA to the College Board upon the conclusion of this Agreement.

Section III.5 How student data is protected:

Access to pupil records is limited to individuals required to access this information as a core job responsibility (support and implementation managers) and is password-protected. Every authorized attempt to access student records is logged for audit purposes.