



# TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678  
Phone (916) 771-1645 • 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 \_\_\_\_\_ (“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 \_\_\_\_\_ 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 \_\_\_\_\_



## TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678  
Phone (916) 771-1645 • 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 \_\_\_\_\_



## TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678  
Phone (916) 771-1645 • Fax (916) 771-1650

*Laura Assem, Director of Technology*

### **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 \_\_\_\_\_



# TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678  
Phone (916) 771-1645 • Fax (916) 771-1650  
*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 \_\_\_\_\_ 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

3/1/2019  
\_\_\_\_\_  
Date

  
\_\_\_\_\_

3/1/19  
\_\_\_\_\_  
Date



## TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678  
Phone (916) 771-1645 • 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) 771-1645 • Fax (916) 771-1650

*Laura Assem, Director of Technology*

See external and internal security measures listed above

---

---

Section II.6 Disclosure notification:

---

---

Section II.8 FERPA compliance:

---

---

Section III.5 How student data is protected:

---

---

Full copy of the text used to fill in the blanks in the agreement:

## **I.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.

### Software Security

Critical Freckle applications undergo regular vulnerability assessments on the running applications (dynamic), the application code (static), and the underlying infrastructure using industry standard tools. These applications also undergo manual penetration testing on an annual basis. The results of these assessments are categorized and prioritized for remediation as swiftly as possible during regular development cycles.

Applications follow a multi-tiered model, which provides the opportunity to apply controls at each layer, practicing "defense in depth." The data centers that house our applications follow industry standard practices and provide an attestation of their annual audits such as SOC Type II.

### Communication Security

All communication with Freckle applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Freckle's email systems utilize state-of-the-art spam and malware filters to prevent outbreaks and phishing campaigns.

---

## **I.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?

### Human Security

All Freckle employees undergo rigorous screening during the hiring process and our contractors are expected to meet the same requirements. All employees must understand and agree to the Information Security Policy. Upon termination or change of employment, access rights are removed or updated to ensure employees only have access to information that is required for their job. Freckle relies on well-defined processes, disciplined execution and continual training of staff, including security and technology use training for employees.

### Physical Security

All Freckle information systems and infrastructure are hosted in a combination of world-class data centers and Infrastructure-as-a-Service (IaaS) providers. All Freckle offices have physical entry controls to ensure only authorized personnel gain access to facilities. Access to facilities is controlled by electronic key systems.

---

## **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

Student-created content is exportable through the teacher and administrator dashboards

---

## **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

If Freckle receives a request to review student data from a student, parent, or guardian, Freckle refer that request to the the school representative within two (2) business days of receiving such a request. Freckle will work cooperatively with the school representative to permit a student, parent, or guardian to review personally identifiable information in student data that has been shared with the Freckle, and correct any erroneous information therein

---

## **II.5**

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

See external and internal security measures listed above.

---

## **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

Upon confirmation of a breach of security that results in the unauthorized release, disclosure, or acquisition of student data, Freckle shall provide initial notice to the school/district as soon as possible, but not more than thirty (30) days after confirmation of such discovery. The Initial Notice shall be delivered by electronic mail to the Data Coordinator and Superintendent, and shall include the following information, to the extent known at the time of notification: 1.Date and time of the breach; 2.Names of student(s) whose student data was released, disclosed or acquired; 3. The nature and extent of the breach; 4.Freckle's proposed plan to investigate and remediate the breach.

---

## **II.8**

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

I. Data in different logically segregated on a per-school basis;



- II. All user accounts have passwords and brute-force login protection;
  - III. Freckle staff accounts are removed as soon as staff members' employment ends; and
- 

### **III.5**

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

Freckle's most important concern is the protection and reliability of our users' data. Our servers are protected by high-end firewall systems, and scans are performed regularly to ensure that any vulnerabilities are quickly found and patched. All services have quick failover points and redundant hardware, with complete backups performed nightly. Access to systems is severely restricted to specific individuals, whose access is monitored and audited for compliance.

Freckle uses Transport Layer Security (TLS) encryption (also known as HTTPS) for all transmitted data. Accounts are protected with passwords and HTTP referrer checking. Our services are hosted in United States by trusted data centers that are independently audited using the industry standard SSAE-16 method.