

**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 \_\_\_\_\_



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

11/2/2017  
\_\_\_\_\_  
Date

Keith Westman, COO  
\_\_\_\_\_  


11/2/2017  
\_\_\_\_\_  
Date

**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:

---

---



## **External Security**

Data is secured using multiple methods. The Otus application can only be accessed by authorized and authenticated users over HTTPS, using a AES 256, TLS 1.2 certificate. Authenticated users can only see data for which they are authorized. Client data is further secured by the AWS Security and Otus' security policies and procedures.

## **Internal Security**

Client data can only be accessed by Otus employees via the application or via a secure, direct connection to the database over SSH, or via files if shared by the district. Only select Otus developers can access the database via a secure, direct connection to the database, using public-key cryptography and username/password. Flat files are securely shared with Otus employees for the sole purpose of importing data into the system.

## **FERPA Compliance**

Under the Family Educational Rights and Privacy Act 1974 (FERPA), schools are required, in some circumstances, to provide parents and guardians with the right to inspect and review the education records of their children and to obtain the consent of the parents or guardians of the student (or the consent of the student, if such student is 18 years of age or older or attending an institution of postsecondary education) prior to disclosing personal information about the student that is contained in the student's education records.

By installing, accessing or using the Services, you represent and warrant that (a) you have read and understand our Privacy Policy and the ways in which Otus collects, uses, and shares information about you in connection with your access to and use of the Services; (b) if you are a Student, you understand that your parent or guardian can view all of the information within or associated with your account and use of the Services, including, without limitation, any messages and other communications between you and your Educator and the grades you received on assignments and other assessments; and (c) the consent of a parent or guardian of the Student (or, if eligible, the consent of the Student) has been obtained by the Student's Educator for the disclosure of information about the Student contained in the Student's education records in accordance with FERPA and any other applicable laws or regulations and our Privacy Policy.

## **Disclosure notification**

We believe the items above cover this, but, please let us know if they don't!

## **How is student data is protected**

If you are installing, accessing or using the Services on behalf of a Student who is under the age of 13, you represent and warrant that (a) you are an authorized Educator who has obtained the consent of the Student's parent or guardian in accordance with the Children's Online Privacy Protection Act of 1998 (COPPA) for the Student's use of the Services, or (b) you are the parent or guardian of the Student and you have provided your consent in accordance with COPPA to your Student's Educator for your Student's use of the Services.

For any questions related to this document, please contact us at [support@otus.com](mailto:support@otus.com)!