

**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

9/8/2016  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Date

9/8/2016

**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:

---

---

## ATTACHMENT

**Roseville City School District  
Educational Technology Services  
Vendor Statement of Compliance for Data Privacy and Protection –  
Supplemental Information**

**Vendor:** Scholastic Inc.

**Product:** Next Step Guided Reading Assessment

**Effective Date:** September 6, 2016,

**Section 1.6:** The systems hosting these services are in a secured private network with hardened load balancers that handle NAT. While there is no IDS, active system monitoring and logging is in place with alarms that are triggered by abnormal traffic behavior.

**Section 1.7:** There is no interaction between vendors and district information unless warranted and approved to determine anomalies in data reporting. District data is entered manually by authorized district personnel and has no interim action required by vendor personnel. Only senior engineers would have access to this data, and again only at the request and approval of district personnel, as designated by the license agreement.

Data is backed up by means of DRDB. Data is maintained in accordance with the duration of the license. Should the district choose to have this data removed from the back end systems written and approved requests need to be submitted through customer service.

**Section 1.8:** An export of student data is available to school and district administrators from within the application. Output is generated to a .csv file.

**Sections 1.9 and 2.7:** License for NSGRA is in perpetuity. Student data is not deleted unless at the request of an authorized agent of the district.

**Section 2.2:** Not applicable.

**Sections 2.4 and 2.6:** Primary responsibility for any communication to or with parents, legal guardians, and students falls upon the agents of the district as the vendor does not have any knowledge of these entities. An agent of the district must contact vendor if district would like to review and/or correct, or would like vendor to facilitate review and/correction by parents, legal guardians or students of, personally identifiable information. If there is an unauthorized disclosure requiring notification, vendor will notify the district, and the district must notify the parents, legal guardians or students.

**Sections 2.5 and 3.5:** Student data is only accessible to those entities within the district that have authorized access (via username/password control) to those accounts in which the student data lives. Additionally, we have a multi-tiered architecture that segregates the applications and data; ensuring each tier is protected using security groups, access control lists, and routing.

**Section 2.8:**

Pursuant to FERPA, the district is responsible to obtain all FERPA-required parental consents and/or to provide all FERPA-required parental notices prior to providing any FERPA-covered pupil records to vendor, and must designate vendor as a “school official” within the meaning of FERPA. Vendor will use any personal information in such pupil records only for the educational purpose for which the district provided the records and will not re-disclose or re-use such personal information for any unauthorized purposes unless it has been de-identified. Vendor may use its own service providers to process or store such personal information, provided such service providers are restricted from disclosing the personal information to any third party or using the personal information for its own purposes or any purpose other than supporting vendor’s operations as necessary for vendor to perform the applicable service or function the district has contracted with vendor to provide. Vendor shall provide district with the names of all such service providers on district’s written request. All pupil records provided by district to vendor hereunder shall remain the property of the district and under its direct control at all times with respect to the use and maintenance thereof.