

## Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Benchmark Education Company, LLC ("Service Provider") on 09/16/2019 ("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

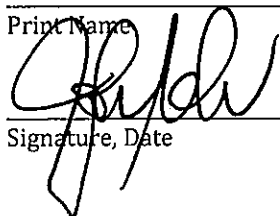
**Section III: SB 1177 SOPIPA Compliance - Student Information Only**

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.

**John Gruber**

Print Name

 1/30/20

Signature, Date

**Laura Assem, 2/6/2020**

Print Name (Roseville City School District)

  
Signature, Date (Roseville City School District)

## EXHIBITS

### Section 1.6: External Security

Benchmark Education follows industry best practices for network and physical security. Please see the attached infrastructure diagram, outlining the security architecture for application deployments.

### Section 1.7: Internal Security

Benchmark has multiple security measures in place to protect the loss, misuse or alteration of information under our control. These include encryption of data in transit, regular software security updates and industry best practices for network and physical security. Data to Benchmark Education is transmitted via OAuth 2.0 over SSL security encryption.

All data is stored in Amazon Web Services (AWS) in the Benchmark Education account. Our Privacy Policy covers the following: handling, use, storage, and retention of Data

In addition to the data security measures described above, limited Benchmark Education staff and select vendor personnel that interact with applications that store student data are required to complete a FERPA/COPPA training certification program before being granted access to those applications.

Data backups are completed on a daily basis, rotated weekly.

Recovery Point Objective (RPO) - data restored within 15 minutes of the time of the event

Recovery Time Objective (RTO) - service restored within 4 hours of the time of the event

### Section II.2: Exporting of Student-Created Content

Student-created content inside Benchmark Universe is saved, stored, and retrieved from inside the platform. This content cannot be exported and/or transferred to a personal account.

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

District personnel are tasked with maintaining the district's user data integrity. Select district technical personnel are granted access to Tech Admin, Benchmark's user data management system. Benchmark will sync and process data changes from one source of truth (e.g. Clever, ClassLink, CSV upload) into Tech Admin. It is the district's responsibility to initiate changes as needed or communicated from parents, guardians, etc.

## EXHIBITS

### Section II.5: Securing Student Data

All data is stored in Amazon Web Services (AWS) in the Benchmark Education account. Benchmark's Privacy Policy covers the following: Handling, use, storage, and retention of Data

The limited Benchmark Education staff and select vendor personnel that interact with applications that store student data are required to complete a FERPA/COPPA training certification program before being granted access to those applications.

Data backups are completed on a daily basis, rotated weekly.

Recovery Point Objective (RPO) - data restored within 15 minutes of the time of the event

Recovery Time Objective (RTO) - service restored within 4 hours of the time of the event

### Section II.6: Disclosure Notification

In the unlikely event that there is an Unauthorized Disclosure of Student Records, we promptly investigate the incident and provide the LEA (Roseville City School District) with detailed information regarding any incident including the identity of affected Pupil Records and Users.

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

Parents do not have direct access to data collected in our platform. Designated School Administrators and District Administrators can access school- or district-level data sets based on their assigned roles in the platform, to then be disseminated to parents. Data sets can be collected in the robust reporting suite, or basic rostering data can be collected in the Tech Admin system.

All BEC personnel with access to personal information are required to complete a FERPA/COPPA certification course before said access is granted. Benchmark Education Company will not share personally identifiable information with any third party without express written consent.

### Section III.5: How Student Data is Protected:

Benchmark has multiple security measures in place to protect the loss, misuse or alteration of information under our control. These include encryption of data in transit, regular software security updates and industry best practices for network and physical security. Data to Benchmark Education is transmitted via OAuth 2.0 over SSL security encryption.

