

**Vendor Statement of Compliance  
Data Privacy and Protection**

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Apex Leadership Company ("Service Provider") on Aug 26, 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

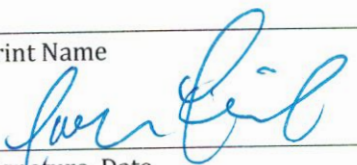
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes  No

As an authorized representative of my organization, I accept the conditions listed in this document.

Jason Freid

Print Name

 8/27/19

Signature, Date

Laura Assem

Print Name (Roseville City School District)



Signature, Date (Roseville City School District)

## EXHIBITS

### Section 1.6: External Security

Our applications are hosted on Microsoft azure's platform as a service and firewalls are managed by Azure.

Here is some documentation on the security

<https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments>

Security advantages of a PaaS cloud service model

Using the same responsibility matrix, let's look at the security advantages of an Azure PaaS deployment versus on-premises.

### Section 1.7: Internal Security

We do not directly access the District data. It is provided via a spreadsheet to us.

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

We do not export Student Created content. Our website does not offer and/or support this feature.

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

-You and your child's school have the right at any time to review your personal information, or that of your child, and have it deleted from the Apex Fun Run System.

-You and your child's school have the right at any time to terminate any further use of your personal information or that of your child.

-In general, we strive to collect personal information by lawful and fair means and in compliance with both Federal and State laws.

- Personal data you provide should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and up-to-date.

## EXHIBITS

### Section II.5: Securing Student Data

- We do not make that personal information publicly available. We use that personal information solely to allow the children, school and/or donors to send e-mails to their friends and family informing them of their participation in an Apex Fun Run and giving such friends and family the opportunity to donate funds. Donor information is not sold or distributed to any third party.
- After the Apex Fun Run pledge and collections process is completed, and all donors have had all their pledge and collections questions answered, donor information is removed from eh site and archived. At this point it is only accessible to Apex home office staff and area managers upon request.

### Section II.6: Disclosure Notification

Your privacy is very important to us. Accordingly, we, Apex Fun Run, LLC, have developed this Policy in order for you to understand how we collect, use, communicate, disclose and make use of personal information. The following outlines our privacy policy.

- Before or at the time of collecting personal information, we will identify the purposes for which information is being collected.
- The information you submit will be collected and maintained by Apex Leadership Co, an Arizona Limited Liability Company, 1 North 1st Street, Suite 790, Phoenix, Arizona, 85004,

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

If Apex will have access to records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the school, or by a party acting for the school ("Education Records"), Apex acknowledges that, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the Education Records and personally identifiable information disclosed to it, and Apex agrees to abide by the FERPA limitations and requirements imposed on school officials. Apex will use the Education Records and personally identifiable information only for the purpose of fulfilling its duties

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

- We will protect personal information by reasonable security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
- We will make readily available to customers information about our policies and practices relating to the management and use of personal information.
- We are committed to conducting our business in accordance with these principles in order to ensure that the confidentiality of personal information is protected and maintained.