RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Accelerate Learning, Inc ("Service Provider") on 08/16/2019 ("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 ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Director of Technology

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 ( )

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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 ◯

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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 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.

Don Keeler
Print Name

8/22/2019
Signature, Date

Laura Assem, 9/23/2019
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Director of Technology

EXHIBITS

Section 1.6: External Security

Iptable, firewalls are implemented. System monitoring for unusual usage. Monitoring of system files.

Section 1.7: Internal Security

ALI utilizes industry-recognized best practices for security. This includes SSL / TLS protocols, API call-level authenti-cation, API bearer tokens, and proprietary solutions. ALI implements the Transport Layer Security (TLS) cryptographic protocol for transfers over HTTPS (SSL) connections. With this protocol, unique session keys are used to encrypt and decrypt data transmissions and validate the accuracy of data transmissions. This process is reinforced by additional proprietary authentication. API calls are authenticated individually using OAuth 2.0 authentication occurring over TLS / SSL protocols. This process is reinforced by additional ALI proprietary authentication. ALI's customer service staff are the only individuals who have access to client data. Staff are trained on how to handle client data, client requests and physical documents. ALI staff only interact with data if the client asks for assistance. ALI's data integration processes are all operated by the client and do not require ALI's assistance. Only appropriate ALI staff have access to client data. All access by ALI and client staff is journaled within ALI's systems. All resources are also protected at the system level. This is protected by standard and non-standard methods with cloud service PCI and SSAE16 certifications.

How is uploaded data from the District handled and processed?
ALI provides several methods of data integration.

ALI's District Master CSV file processing utilizes SFTP (Automated and Interactive) Each SFTP area is specific to each client and is not a shared resource. Uploaded files are immediately moved to an internal, isolated area for secure processing.

Other Options;
IMS Global – OneRoster (REST, CSV)
Aeries SIS
Schoology
Canvas

ALI also offers an alternative student/sis data integration solution through IMS Global's OneRoster.

Who has access to this data?
ALI customer support and client staff.

What happens to the data after the upload is complete?
Uploaded files are immediately moved to an internal, isolated area for secure processing.

Section II.2: Exporting of Student-Created Content

The system allows for a students assessment scores to be exported from the system.

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

Parents may use their student's account to access their student's information. Student ID, School, Student Name and Grade Level are the only required fields. Any changes to this information have to be reported to the district, as it provides and maintains all student information used within the system.

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Districts are able to manually enter their data directly into the system, or merge their information through data file submissions. Staff using their district assigned user id and passwords complete these tasks. The school district's personnel prepare student import files that are submitted to the system. These files are processed through a private, secure SFTP area that is not shared with any other resource. All actions can be performed without the assistance of ALI staff. Appropriate District Administrative personnel are provided training on the maintenance of student data through the ALI portal. District Technical staff are provided with detail setup information from their portal access. If a district's technical staff requires assistance, they have access to contact ALI's technical support.

Section II.6: Disclosure Notification

ALI will first verify a breach has occurred. Upon verifying the event, ALI will contact by phone the appropriate district personnel. A full report of the incident will be emailed to the staff member as well.

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

ALI meets all requirements of FERPA. Modifications to student records are logged and available for appropriate district staff to review. A district is able to maintain student records manually to make modifications. ALI intentionally requires minimal information, all of which is typically defined by District's as "Directory Information". (Title 20 › Chapter 31 › Subchapter III › Part 4 › § 1232g) If District personnel have any questions, or concerns, regarding FERPA compliance, they may contact ALI Technical Support.

Section III.5: How Student Data is Protected:

ALI utilizes industry-recognized best practices for security. This includes SSL / TLS protocols, API call-level authenti-cation, API bearer tokens, and proprietary solutions. ALI implements the Transport Layer Security (TLS) cryptographic protocol for transfers over HTTPS (SSL) connections. With this protocol, unique session keys are used to encrypt and decrypt data transmissions and validate the accuracy of data transmissions. This process is reinforced by additional proprietary authentication. API calls are authenticated individually using OAuth 2.0 authentication occurring over TLS / SSL protocols. This process is reinforced by additional ALI proprietary authentication. ALI's customer service staff are the only individuals who have access to client data. Staff are trained on how to handle client data, client requests and physical documents. ALI staff only interact with data if the client asks for assistance. ALI's data integration processes are all operated by the client and do not require ALI's assistance. Only appropriate ALI staff have access to client data. All access by ALI and client staff is journaled within ALI's systems. All resources are also protected at the system level. This is protected by standard and non-standard methods with cloud service PCI and SSAE16 certifications.