



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 for Data Privacy and Protection

This agreement is entered into between Roseville City School District (“LEA”) and Amplify Education, Inc. for K-8 Amplify Science (“Service Provider”) August 5, 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



TECHNOLOGY SERVICES

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



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 ___X___ 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 ___X___ No _____
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract
Agree: Yes X_____ 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 ___X___ No _____
5. Vendor will attach to this document evidence how student data is kept secure and confidential
Agree: Yes ___X___ 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 ___X___ 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 ___X___ No _____
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA
Agree: Yes ___X___ 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 ___X___ No _____



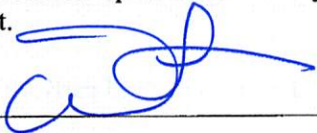
TECHNOLOGY SERVICES

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 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

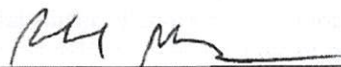
As an authorized representative of my organization, I accept the conditions listed in this document.



Roseville City School District

8/5/19

Date



Amplify Education, Inc.
Richard Morris, Chief Financial Officer

08/05/2019

Date



TECHNOLOGY SERVICES

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

Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

Amplify maintains a comprehensive security program, as described in the attached security statement. Sections 4 (Application Security by Design), 5 (Proactive Security), and 6 (Reactive Security) are all directly relevant to external security.

Amplify undergoes annual third party security examinations, including SOC 2 Type 2 examination. Examination results are available upon request.

Section I.7 Internal Security:

Amplify maintains a comprehensive security program described in the attached security statement. Sections 2 (Policies & standards), 3 (Data access controls), and 7 (Compliance) are all directly relevant to internal security.

On the specific questions:

- Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed?
 - Depending on the data integration model chosen during the implementation process, District roster data is uploaded directly by the District to an Amplify secure file transfer service, or uploaded by the District to an integration partner such as Clever. Amplify personnel review the completion and integrity of the data flow, then enable automated processing of roster data.
- Who has access to this data?
 - Amplify's access control principles dictate that all student personal information we store on behalf of customers is only accessible to district-authorized users and to a limited set of internal Amplify users who may only access the data for purposes authorized by the district. Districts maintain control over their internal users and may grant or revoke access.
 - In limited circumstances and strictly for the purposes of supporting school districts and maintaining the functionality of systems, certain Amplify users may access Amplify systems with student personal information. All such access to student personal information by Amplify technicians or customer support requires both authentication and authorization to view the information.
- What happens to the data after the upload is complete?
 - While the details depend on the data integration model chosen during the implementation process, District roster data is deleted from intermediate storage after synchronization to Amplify systems is complete.
- What security safeguards are in place to protect unauthorized access to District data?
 - See the attached Security Statement.
- 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"?
 - Amplify backs up customer data regularly (at least daily) to AWS S3, which provides 99.999999999% durability across multiple facilities, as described at <https://aws.amazon.com/s3/faqs/>. Data backups are regularly tested.
 - Data backups are stored within production environments, with access restricted to a limited set of internal Amplify users to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the district.
 - Personally identifiable information in backups is encrypted using the industry-standard AES-256 encryption algorithm.



TECHNOLOGY SERVICES

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

Laura Assem, Director of Technology

- Data backups are maintained for at least 30 days.
- Backups are regularly destroyed on appropriate schedules.
- If any data is printed, what happens to these hard copy records?
 - We will retain personal information collected from our School District and SEA customers for the period necessary to fulfill the purposes outlined in this Policy and our agreement with that School District or SEA customer. Specifically, at the direction of our customers, Amplify will return or destroy personal information stored by Amplify in accordance with applicable law and customer requirements.

Section I.7 District Access

Upon request, Amplify can provide larger-scale secure exports of student data on a periodic basis, not to exceed quarterly. Data formats include CSV and JSON.

Section II.2 Exporting of student created content:

Teachers can one-click export student scores from each lesson in CSV format, and student work in printable formats. Upon request, Amplify can provide larger-scale exports of student performance data on a periodic basis (see I.7).

Section II.4 Review and correcting personally identifiable information:

See attached Amplify Customer Privacy Policy.

FERPA requires schools to provide parents with access to their children's education records, and parents may request that the school correct records that they believe to be inaccurate or misleading. If you are a parent or guardian and would like to review, correct or update your child's personal information stored in our product or service, contact your School District. Amplify will work with your School District to enable your access to and, if applicable, correction of your child's education records.

If you have any questions about whom to contact or other questions about your child's personal information, you may contact us using the information provided below.

Section II.5 Securing student data:

Please see attached Information Security document.

Section II.6 Disclosure notification:

Please see attached Amplify Customer Privacy Policy.

In the event Amplify discovers or is notified of an unauthorized disclosure of personal information within our possession or control, we will, as required by applicable federal and state laws, investigate, take steps to mitigate the potential impact, provide notice of the breach to applicable agencies, including School District and SEA Customers.

Section II.8 FERPA compliance:

Please see attached Customer Privacy Policy.

Section III.5 How student data is protected:

Please see attached Amplify Customer Privacy Policy and Information Security document.