Roseville City School District

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • 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 5-Star Students,LLC ("Service Provider") on 3/23/2018 ("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 X 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 X 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 X No _____

Roseville 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 X 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 X 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 X 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 X 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 X 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 X 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 X No _____

Roseville City School District

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • 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 _____ No N/A

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 _____

Roseville City School District

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • 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 X No _____
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract
   Agree: Yes X No _____
3. Vendors cannot sell student information
   Agree: Yes X No _____
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons
   Agree: Yes X No _____
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices
   Agree: Yes X No _____
6. Vendors must delete district-controlled student information when requested by the school district
   Agree: Yes X No _____
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
   Agree: Yes X No _____

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

_____ 3/23/2018

Roseville City School District — Date

_____ 3/23/2018

Brian Bourgeois, Managing Member — Date

Roseville City School District

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1600 • Fax (916) 771-1650
Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

(see attachment)

Section I.7 Internal Security:

(see attachment)

Section II.2 Exporting of student created content:

(see attachment)

Section II.4 Review and correcting personally identifiable information:

(see attachment)

Section II.5 Securing student data:

Roseville City School District

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:

(see attachment)

Section II.8 FERPA compliance:

(see attachment)

Section III.5 How student data is protected:

(see attachment)

Roseville City School District: Vendor Compliance Exhibits

Section I.6 External Security:

All data collected through the Service is stored and processed in the United States. Our service is hosted on the Microsoft Azure cloud platform, which provides DDoS protection, NAT endpoints, and monitoring capabilities. Databases are located behind firewalls that require user/password credentials and pre-authorized IP-addresses

Section I.7 Internal Security:

We maintain strict administrative, technical and physical procedures to protect information stored within our system. Access to information is limited (through user/password credentials and IP-address) to only those employees who require it to perform their job functions. We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and connectivity to the Service. There is no means of self-registration to gain instant access to the system, it is by invitation only. Other security safeguards include but are not limited to data encryption and firewalls. Data is uploaded to the Service through a web interface, by authorized LEA users only (i.e. school personnel). Data backups are taken using geo-redundant storage and kept for a period of 35 days. Backups are encrypted and saved within a secure storage area and only accessed in case of disaster recovery scenarios.

Section II.2 Exporting of student created content:

Student data is created solely by LEA users. There is no pupil-generated content

Section II.4 Review and correcting personally identifiable information:

Students and/or parents/legal guardians may review data held by our Service, using the included “school web page” option. Authorized school site administrators can enable the web page option, hosted by the Service, and allow individuals to view their data using a designated authentication method. As there is no pupil-generated content, individuals must request any corrections directly through the applicable School or LEA. We have no ability to evaluate the merits of requests for data corrections by students or their parents/legal guardians.

Section II.5 Securing student data:

We consider LEA's Student Data as confidential and does not share it with third parties. We may disclose or provide access to Student Data to employees and certain service providers with a legitimate need to access such information in connection with providing the Services. Our employees, subcontractors, or agents involved in the handling, transmittal, and/or processing of Student Data will maintain the confidentiality of any data that includes personally identifiable information and shall not redisclose such data except as necessary in order to provide the Services. Student Data is controlled by LEA and we cannot permit anyone else to delete or control Student Data or to transfer such content, or allow direct access to Student Data by parents or legal guardians; as such, we will refer any data access requests to LEA.

Section II.6 Disclosure notification:

If there is any disclosure or access to personally identifiable Student Data by an unauthorized party, we will promptly notify LEA and will use reasonable efforts to cooperate with their investigations of the incident. The notification will include as much information as possible about the nature of the disclosure and our steps to mitigate the situation. If the incident triggers any third party notice requirements under applicable laws, you agree that, as the owner of the Student Data, LEA will be responsible for the timing, content, cost, and method of any required notice and compliance with those laws.

Section II.8 FERPA compliance:

Pupil Data is any information (in any format) that is directly related to any identifiable current or former student that is maintained by LEA and may include “educational records” as defined by the Family Educational Rights and Privacy Act ("FERPA"). While we may need to access Pupil Data to provide the Services to LEA, LEA owns the Pupil Data and remains responsible for it. Site administrators/managers appointed by LEA (each School) control the type of information that is accessible within the Service to ensure that all users are assigned the least-privileged role for achieving their objectives in the system. The Service requires that anyone desiring system access must contact site manager(s) and be invited to create an account. There is no means of self-registration to gain instant system access. All access to the Service is logged and includes information such as IP Address, user ID, success/failure of the login, and the role assigned when accessing the system. This log information is available to the LEA upon request. The system is proactively monitored by advanced monitoring services provided by an independent network security provider. Our technical staff also periodically reviews instances of failed login attempts. No personally identifiable Pupil Data can be made public from the system in any capacity. All access to Pupil Data is available to authorized users only. Individual requests to have Pupil Data expunged from our service, must be initiated through the LEA as we have no ability to evaluate the merits of such requests. We can assist the LEA with such requests on a case-by-case basis through normal support channels.

Section III.5 How student data is protected:

User accounts provide access to the Service and associated Student Data. The Service maintains different types of accounts for different user roles. There is no means of self-registration to gain instant access to the Service. Individuals may be invited by authorized LEA administrators/managers to create an account with a specific level of access. LEA is responsible for any activity that occurs within LEA's user accounts. Individuals with access to LEA's Student Data must never use someone else’s account without permission and must keep account passwords secure. We recommend using “strong” passwords (passwords that use a combination of upper and lower case letters, numbers and symbols) with user accounts to avoid unauthorized use. LEA must advise us immediately if user account security has been compromised. No personally identifiable Student Data can be made public from the system in any capacity. All access to Student Data is available to authorized users only.