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, Executive 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 Allen Eubank BOSS App ("Service Provider") on 8/1/2024 ("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.

Allen Eubank
Print Name

8/1/2024
Signature, Date

Laura Assem
Print Name (Roseville City School District)

8/5/2024
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

The BOSS app prioritizes security through a device-centric approach. Key features include: offline functionality with local data storage, secure coding practices, minimal data collection (anonymous usage analytics only), and no personal identifiable information stored. We leverage built-in device security features and recommend their use. Our development process includes threat modeling, secure code reviews, and rigorous testing. An incident response plan is in place for addressing potential issues. By focusing on local storage and minimal data collection, we've created a system resistant to external compromise while maintaining core functionality.

Section 1.7: Internal Security

The BOSS app stores all data locally on the device, with no uploads or external transmissions. Our personnel never access district data. All processing is done on-device, with access limited to authorized users. We don't perform backups or offer printing. This design eliminates risks of unauthorized access, ensures data remains under district control, and maintains the highest level of privacy and security.

Section II.2: Exporting of Student-Created Content

The BOSS app doesn't handle student-created content. It's designed for practitioners to record behavioral observations, not for students to create or store their own work. Therefore, there's no student-created content to export or transfer. All data in the app is inputted and managed by authorized school staff.

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

The BOSS app doesn't store personally identifiable information (PII) about students or parents. It only contains behavioral observation data input by school staff. Since there's no PII to review or correct, this requirement doesn't apply to our app. Schools maintain full control over the data and can manage it according to their policies.

EXHIBITS

Section II.5: Securing Student Data

The BOSS app ensures data security and confidentiality by: storing all data locally on the device, never transmitting data externally, utilizing device-level encryption, implementing strong in-app authentication, collecting no personally identifiable information, and allowing offline functionality. This approach keeps student data under direct school control, eliminating risks associated with data transmission or third-party access.

Section II.6: Disclosure Notification

As the BOSS app stores all student data locally on the device and never transmits it externally, there is no risk of unauthorized disclosure of student records from our servers or systems. In the unlikely event of a device breach or loss, we recommend schools follow their existing protocols for notifying affected parties, as they retain full control and responsibility for the data. We can provide guidance on best practices for device security and data protection upon request.

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

The BOSS app is designed to be FERPA compliant by default. We do not collect, store, or transmit any student records or personally identifiable information. All data remains locally on the school's device, under their control. We have no access to student information and do not share any data with third parties. This approach ensures that schools maintain full compliance with FERPA regulations while using our app.

Section III.5: How Student Data is Protected:

The BOSS app protects student information through several security measures: local data storage on the device with no external transmission, reliance on built-in device encryption, strong in-app authentication, minimal data collection (no personal identifiable information), offline functionality, regular security audits, secure coding practices, and an incident response plan. These procedures ensure that student data remains under school control and is protected from unauthorized access or breaches.