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 ClassDojo ("Service Provider") 4/23/2018 ("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 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 _____

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.

_____ 4/23/2018

Roseville City School District — Date

_____ 04 / 23 / 2018

Meg Bowman, ClassDojo — 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:

Section I.7 Internal Security:

Section II.2 Exporting of student created content:

Section II.4 Review and correcting personally identifiable information:

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:

Section II.8 FERPA compliance:

Section III.5 How student data is protected:

Section I.6 External Security:
The security of your personal information is important to us. We work hard to protect our community, and we maintain administrative, technical and physical safeguards designed to protect against unauthorized use, disclosure of or access to personal information. In particular:

- Our engineering team is dedicated to keeping your personal information secure
- We work with a team of security researchers to continually test ClassDojo' s security practices for vulnerabilities
- We periodically review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems
- We continually develop and implement features to keep your personal information safe - for example, when you enter any information anywhere on the Service, we encrypt the transmission of that information using secure socket layer technology (SSL/TLS) by default
- We ensure passwords are stored and transferred securely using encryption and salted hashing
- The ClassDojo Service is hosted on servers at a third-party facility, with whom we have a contract providing for enhanced security measures. For example, personal information is stored on a server equipped with industry standard firewalls. In addition, the hosting facility provides a 24x7 security system, video surveillance, intrusion detection systems and locked cage areas.
- We automatically delete inactive student accounts after a specific period of time, as per our retention policy, described in the "How Long Does ClassDojo Keep Children's Information?" section
- We also operate a 'bug bounty' security program to encourage an active community of third-party security researchers to report any security bugs to us. More information on this is available by contacting us at privacy@classdojo.com.

Network security
ClassDojo ensures security at the network level using SPI firewalls, hardened bastion hosts and end-to-end 2048-bit TLS/SSL encryption across all our networks.

Infosec governance
ClassDojo enforces regular security and privacy training for employees, and employs very strict policies, access controls and auditing around internal access to our systems.

Application security
ClassDojo follows published secure application coding practices, verified by an exhaustive suite of automated tests, as well as regular code reviews and testing by independent researchers.

Rigorous audits

Extensive third-party audits by world-class firms like the NCC Group ensure we are constantly putting ClassDojo systems and protocols under extreme, unbiased scrutiny.

Section I.7 Internal Security:

- Employees are only allowed access to user information if required for providing support to the user(s) themself, or debugging an issue. Access is done over secure connections.
- Employees go through background checks.

Section II.2 Exporting of student created content:

- Authorized individuals can request student created content by emailing our Success team at hello@classdojo.com.

Section II.4 Review and correcting personally identifiable information

- Authorized individuals can request, review, and correct personally identifiable information within the app under Settings, or by emailing our Success team at hello@classdojo.com.

Section II.5 Securing student data:

Refer to response in *Section I.6 External Security*. Additionally, only the student, their teacher(s), and their own guardian(s) can review student information.

Section II.6 Disclosure notification:

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time. If we learn of a security breach, we will attempt to notify you electronically (subject to any applicable laws) so that you can take appropriate protective steps; for example, we may post a notice on our homepage (www.classdojo.com) or elsewhere on the Service, and may send email to you at the email address you have provided to us as a user or district leader.

Section II.8 FERPA compliance:

ClassDojo holds the iKeepSafe FERPA Certification signifying its Website and Apps have been reviewed and approved for having policies and practices that are compliant with the federal mandates for FERPA.

Section III.5 How student data is protected:

In addition to the security measures shared above, we protect student information by allowing students (and their guardians) to always access their information for free, either by using the app or by contacting us directly at hello@classdojo.com. Furthermore, we only keep a child's personal information for as long as his or her student account is active, unless we are required by law to retain it, need it to ensure the security of our community or our Service, or to enforce

our Terms. More specifically, ClassDojo operates a 3-tier student data protection policy to protect all students' (not just children's) information ("3-Tier Student Data Protection Policy"). Read more about that here: https://www.classdojo.com/privacy/#HowLongDoesClassDojoKeepChildrensInformation