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 **Keyboarding Without Tears** ("Service Provider") **January 7, 2016** ("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.

Laura Assem _____ 2/26/2016

Roseville City School District — Date

_____ 02/25/2016

Keyboarding Without Tears — 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 Letter

Section I.7 Internal Security:

See Letter

Section II.2 Exporting of student created content:

See Letter

Section II.4 Review and correcting personally identifiable information:

See Letter

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

See Letter

Section II.6 Disclosure notification:

See Letter

Section II.8 FERPA compliance:

See Letter

Section III.5 How student data is protected:

See Letter

No Tears Learning, Inc.

Date: 02/25/2016

Laura Assem, Director of Technology
Roseville City School District
1050 Main Street | Roseville, CA 95678
Office: (916) 771-1600 Ext. 141

Dear Ms. Laura Assem,

Pursuant to the agreement between Roseville City School District and Keyboarding Without Tears (KWT) that was executed on January 7, 2016, we provide the following responses to the relevant sections of the *Vendor Statement of Compliance for Data Privacy and Protection (*the "Vendor Compliance Statement"*).*

To be sure, we state that KWT complies with the legal requirements and policy stipulations in every subsection of *Section I: General*, *Section II: AB1584 Compliance*, and *Section III: SB 1177 SOPIPA Compliance*. Particular subsections within various Sections of the Vendor Compliance Statement requested additional descriptions and documentation. They are provided below.

Section I: General

- **I.6: EXTERNAL SECURITY**
  - We have taken the necessary steps to ensure that the servers on which our system runs are secure from external hacking and attacks. We require HTTPS and SSH for all communication to our servers, including for private API/web services. Only selected ports are open as needed. All access to all databases and servers are secured by firewall rules (by IP address, port, and protocol). See Exhibit A – KWT Security Overview.
- **I.7: INTERNAL SECURITY**
  - We have taken necessary steps to ensure that the servers on which our system runs are secure from internal hacking and attacks. Concerning the access to District data, we do not share any data with external vendors. We perform backups of the data. We require HTTPS and SSH for all communication to our servers, including for private API/web services. Only selected ports are open as needed. All access to all databases and servers are secured by firewall rules (by IP address, port, and protocol). See Exhibit A – KWT Security Overview. We perform weekly restores on secure servers within our in-house IT infrastructure.
  - District data/roster changes are applied to our secure, hosted database in multiple methods depending on the customer's preference:
    - a.) Manually entered through the PlusLiveInsights Digital Dashboard interface.

        - b.) A one-time, bulk import process provided using a CSV file from the customer.
        - c.) Integration through Clever.com's roster management approach, where we and the customer synchronize roster changes on a periodic basis (usually nightly).
    - The secure, hosted database is only accessible to our application servers and a 'Bastion' server, which allows only limited access from our headquarters for maintenance purposes. Standard firewall rules are applied to all servers in the infrastructure, including account, port and IP address restrictions.
    - Backups are maintained in a secure, hosted location and kept for 7 days (online) by day of week. We maintain monthly backups at our on-site location indefinitely.

- **I.8 DISTRICT ACCESS**
    - We provide a secure means for the District to extract all data from our system upon request. Once a District submits a request for data extraction including the relevant parameters to pull this data from our system's data warehouse, we will make the data extraction in the form of a compressed file of the customer data. The compressed files will be in CSV format, containing teacher, class, student, and student progress data.

Section II: AB1585 Compliance

- **II.2**
    - Roseville City School District may request a copy of any student created content by contacting our Customer Support team on an ad hoc basis. Upon request, we will establish account credentials for the customer to login to a secure server and download the compressed CSV file(s) within a reasonable timeframe, such as 24-48 hours from the request submission.
- **II.4**
    - Upon request, we provide parents, legal guardians and students the ability to review and correct their personally identifiable information (PII). A parent, legal guardian, or student may contact our Customer Service department and submit a request for such review. Once the request is submitted, our Legal Department and in-house Information Technology Department reviews the request, verify the correctness of PII. If the PII is incorrect, we make the proper corrections and provide notice to the District and the submitter of the request that such a request was submitted and addressed. Noteworthy, the KWT application currently only requires a student first name and last initial. No other personal identifiers are required or stored. Teacher information requires a valid e-mail address. Standard +Live Insights ("+LI") users (e.g. teachers) may maintain the student names via +LI user interface. Clever customers do not have the ability to update Student information, including rostering.

- These requests are currently handled by exception when a customer contacts Customer Service. There is no function to provide this through the application or the +LI dashboard, except for non-Clever customer teachers being able to change the student first and last name. Clever customers may do this at anytime by contacting their school to have the Student Information System (SIS) updated which will be applied to the KWT database within a 24-hour period of the school updating their SIS/Clever information so the change would be maintained in the SIS and trickle down to +LI via the Clever synchronization process.

- **II.5**
  - Our student data is kept secure and confidential as a result of our compliance with *I.6: External Security* and *I.7 Internal Security* in Section I and with the compliance of our policies with the Federal Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 C.F.R. Part 99. The data is secured with firewall rules and limits which servers can access the database, which are a complex of servers configured, secured, operated and maintained by us. The student identifiable information is never shared outside of the intended application usage, and is secure as aforementioned. Student identity is contained in a single database table, and de-identified in all other cases of reference. The student first and last name are used exclusively by the application for personalization and for the student to select their name during login (for standard +LI and at-home users only). See Exhibit A – KWT Security Overview.
- **II.6**
  - If ever an unauthorized disclosure of student records occurs, our Legal Department will promptly follow KWT's data breach policy response protocol. Within this protocol, the first step is validating the data breach, including examination of initial information and server and application logs to confirm that the breach has occurred, including identification of the information disclosure and method of disclosure (internal/external disclosure, malicious attach, or accidental). After the data breach has been validated, step two of our protocol assigns an incident manager responsible for investigation who in addition to investigative activities, also produces breach response documentation. Step three of our protocol assembles an internal incident response team that determines if the status of the breach is on-going, active, or post-breach, whereby such status defines corresponding actions required to prevent further data loss by securing and blocking unauthorized access to systems/data and associated mitigation efforts. Step four of the protocol determines the scope and composition of the breach, including the identification on all affected data, machines, and devices, and location, obtainment, and preservation of all written and electronic logs and records applicable to the breach for examination. Step five of the protocol reaches out to the data owners, in this context, the affected parents, legal guardians and/or eligible students. Step six of the protocol works

with the District to notify the Family Policy Compliance Office (FPCO) of the breach to aid in the determination of the resulting potential harm caused by the unauthorized disclosure.

- **II.8**
    - **FERPA.** In compliance with the Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), and with regard to the availability of KWT in schools in the United States, we are first granted lawful access to directory information (specifically, student names) from student education records by school officials with legitimate educational interest in American public schools. We subsequently utilize students' names for the specific purpose of delivering KWT's suite of digital products and services to students with KWT licenses in those public schools. As part of our service provided to the District, we also run reports associated with student names to indicate the number of KWT activities completed, days in use, and student performance reports based on KWT Spot Check metrics. With regard to the rights that FERPA confers to parents or eligible students to inspect, review, correct, or otherwise access student education records maintained by public schools and shared with us by school officials with legitimate educational interest, we will cooperate with schools officials to ensure that the rights of parents and eligible students under FERPA, and the security of student education records are protected. KWT is fully compliant with FERPA. Specifically,
        - Any sensitive online information is transmitted over secure, encrypted channels via Secure Socket Layer (SSL) as well as other layers of encryption.
        - All student data is stored on secure servers utilizing encryption and firewall technology and are not publicly accessible.
        - All student-related progress data is stored in an aggregated, anonymized, or non-identifiable format that is untraceable to individual students.
        - KWT will not share a student's personally identifying information with third-parties.
    - **PII.** In the course of providing educational products and services to you, we may at times request and temporarily store certain types of personally identifying information about students in order to enable student login and student license-based access to selected applications in our suite of digital products and services. We adopt the definition of personally identifiable information set forth under the FERPA regulations, pursuant to 34 CFR § 99.3 ("Personally identifiable information"). We consider the following to be examples of personally identifying information: first and last name, grade, gender, date of birth, school name, parental e-mail, a personal identifier such as a student's social security number or student number, or any other information that would make the student's identity easily traceable. We will not require a student to disclose more personally identifiable information than is reasonably necessary to participate in online activities. In the scenario in which a student may enter

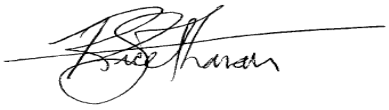
personally identifying information, we ask parents and educators to help us protect the privacy of students by instructing them never to provide personally identifying information without getting parental/guardian or teacher permission first.

Section III: SB 1177 SOPIPA Compliance

- **III.5** The student data is secured with firewall rules and limits which servers can access the database, which are a complex of servers configured, secured, operated, and maintained by us. The student identifiable information is never shared outside of the intended application usage, and is secure as aforementioned. Student identity is contained in a single database table and de-identified in all other cases of reference. See Exhibit A – Security Overview.

If you have any further questions or concerns, please feel free to contact me.

Best,



Rajeev Sreetharan
In-House Counsel

o.301.263.2700 x126
c.240.606.1147
Rajeev.Sreetharan@hwtears.com

Exhibit A: Keyboarding Without Tears (KWT) Security Policy

Software Security

Data Transmission

Communication between a client application and our backend servers is via a secure, private API requiring the use of a proprietary, dynamic security token for all web service calls.

API Calls

All web service calls are made over HTTPS using TLS cryptographic protocol. This ensures integrity of the data being transmitted; using unique session keys to encrypt/decrypt the data over the wire. Each web service call is also stateless, meaning authorization must be made by each subsequent service call, due to not storing any relevant 'state' information on the servers to link web service calls to a specific API client.

User Data Isolation

As data enters into the database, the particulars used to positively identify a user (teacher or student) are isolated as much as possible and replaced with synthetic identifiers used throughout the data model. The user elements retained, such as student name or teacher name to make the applications effectively usable.

During normal use of the application, these identifiable elements are visible via the applications by the user with proper access credentials. Upon terminated of the contract and written request from the customer, these elements are permanently destroyed.

Student Identifiable Information

As much as possible, a minimal amount of Student identifiable information is maintained in the database exclusively and expressly for the purposes of student login (authentication) and application personalization. Such information currently only includes student firstname, lastname, grade and optionally parent(s) email addresses. Upon entry into the database, the Student Identifiable Information is assigned a synthetic ID used through all operations and reporting with in the system. The Student Identifiable Information may be destroyed upon written customer request.

Facility Security

The data centers used to operate our infrastructure are run by industry leading providers with decades of experience designing, building and running highly available facilities with multiple, redundant paths for power, networking, physical and virtual security facilities.