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 EduTyping/Educademy LLC ("Service Provider") 05/25/2018 ("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 ✓ 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 _____

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 ✓ 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 _____

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 ✓ 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 _____

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 ✓ 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.

Laura Assem — 5/28/2018

Roseville City School District — Date

Joshua J. Bruce — 05/25/2018

Date

EduTyping
A Teaching.com Product

Exhibits

Section I.6 External Security:

The EduTyping Support Team proactively monitors any possible vulnerabilities or acts of intrusion. If a vulnerability is detected, then our highly skilled team of developers deploy a patch to all our systems using a single docker image. The team restricts Shell access through generic internet use by requiring all individuals to log into a VPN. Then, the team isolates the intrusion and places it into a "container" where it can be permanently exterminated. Additionally, EduTyping provides Roseville City School District protection from Cloudflare.

Section I.7 Internal Security:

Access to stored information is restricted to EduTyping's CEO, Operations Team, and Lead Developers. Information is never altered, replaced, deleted, or added with the express permission of the user. EduTyping does not allow Shell access to any web applications. They are isolated on docker containers and servers are never exposed to the internet. The only way to obtain access is to go directly through the VPN. Containers are recycled every few hours. We have daily automated backups for databases and we also version control all code releases. This ensures that easy recovery is possible when/if a catastrophic failure occurs. Additionally, we have multi-zone, point-in-time recovery for each of our databases in case of unforeseen natural event(s). Cloudflare DDoS Firewall is our protection against denial-of-service attacks. Data is uploaded in 1 of 4 ways: individual student upload, batch uploading, CSV file uploads, or Clever integration. All data is deleted upon the termination of contract.

Section II.2 Exporting of student created content:

Student data can be exported directly within the EduTyping platform. A teacher, admin, or district admin has the authority to do so by logging into their own individual portal. The reporting function allows different reports to be run and saved. However, one can export all data at one time by simply clicking the "My Account" tab.

Section II.4 Review and correcting personally identifiable information:

The only entity that will have access to review or change personally identifiable information will be the individual instructor, admin, or district admin. EduTyping does ask that students log into the portal using a username and password created by any of the individuals listed above. Personally identifiable information that may be collected include first names, last names, and emails. However if the Roseville City School District would like to opt out of this option, then generic usernames and passwords may be generated.

Section II.5 Securing student data:

All information including student data is securely stored within the continental US. EduTyping utilizes an internal network to transmit information/data to a relational database (RDBMS). All of the above described activity takes place on a private subnet without internet access. Data such as passwords are encrypted with a unique environment-based key while at rest. When the data is in transit, EduTyping uses SSL encryption.

Section II.6 Disclosure notification:

EduTyping manages data breaches by employing dedicated Development Operations team members that are tasked with overseeing and managing security 24/7 throughout the year. These team members are responsible for monitoring and responding to any security threats, including those related to data breaches. Additionally, EduTyping restricts Shell access through Secure Shell (SSH) use by requiring all individuals to log into a VPN. This enables our team to isolate intrusions and breaches by placing them into "containers" to be permanently exterminated. If there is a data breach, then EduTyping will notify Roseville City School District and work together to appropriately notify affected parents, legal guardians or eligible students.

Section II.8 FERPA compliance:

EduTyping is compliant with the Family Educational Rights and Privacy Act. The only student information obtained via EduTyping would be with the express permission from Roseville City School District. System Administrators from Roseville City School District using the EduTyping platform will have the authority to share student information, but EduTyping will not disseminate such data unless in accordance with parties outlined in the Family Educational Rights and Privacy Act.

Section III.5 How student data is protected:

a. All information is specifically housed in the us-east-1 (Virginia) Region. Information and Data are transmitted via internal network to a relational database (RDBMS). This takes place on a private subnet without internet access. Passwords are encrypted with a unique key that is based on the environment. Each environment is provided with an individualized hash key that is utilized for password encryption. EduTyping uses SSL encryption to protect all in-transit data. All systems are located on Amazon Web Services (AWS). AWS operates under constant vigilance and continuously works to improve security.