TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • 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 **Illuminate Education, Inc.** ("Service Provider") **April 1, 2019** ("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 _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • 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 _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • 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 X

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 _____

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • 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.

_____ 3/29/2019

Roseville City School District — Date

Deanna Kulajian 3/29/2019

Illuminate Education, Inc. — Date

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

Exhibits

Section I.6 External Security:

See attached Data Security document.

Section I.7 Internal Security:

See attached Internal Security Section 1.7 document.

Section II.2 Exporting of student created content:

Not applicable.

Section II.4 Review and correcting personally identifiable information:

Illuminate directs all students and/or parents to the District to review and correct any erroneous data. Illuminate products are designed to give the District full control over access to data and regulation of the data uploaded to our platforms, and as such, the District is the exclusive party for permitting a student and/or parent the ability to review and correct data.

Section II.5 Securing student data:

TECHNOLOGY SERVICES

1050 Main Street • Roseville, CA 95678
Phone (916) 771-1645 • Fax (916) 771-1650
Laura Assem, Director of Technology

See attached Data Security Document

Section II.6 Disclosure notification:

Illuminate notifies customers (generally the school or district) as quickly as practical and the customer will determine how best to communicate to any impacted students or parents.

Section II.8 FERPA compliance:

See attached Data Security Document.

Section III.5 How student data is protected:

See attached Data Security Document.

INTERNAL SECURITY Section I:7
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.

During the initial data implementation members of the vendor's data services team will work directly with District data files to support the import process. Data files from the District are always submitted to the vendor via SFTP.

How is uploaded data from the District handled and processed?

After the initial data implementation is complete all uploaded data from the District is handled and processed through the data automation processes. There is no manual handling or manipulation of data once the automation processes are underway.

Who has access to this data?

Members of the vendor's data services and support teams have access to the vendor's SFTP server. Data is only accessed to address data support issues.

What happens to the data after the upload is complete?

The files used to upload the data remain on the SFTP server indefinitely.

What security safeguards are in place to protected unauthorized access to District data?

Data is uploaded to secure SFTP. Each customer's data is stored in it's own database. Access to production databases is restricted to authorized Illuminate personnel only. All data is encrypted at rest and in transmission.

How are backup performed and who has access to and custody of the backup media?

Backups are automatically performed every day. Access and custody of the backups are maintained by the Hosting Operations team within Illuminate. Copies of the backup files are available upon request.

How long are backup maintained; what happens to the District data once the backup is "expired"?

Backups are stored indefinitely and do not expire. The MSA outlines the terms of Illuminate's responsibility to remove client data backups from the servers upon expiration of an agreement between the customer and Illuminate.

If any data is printed, what happens to these hard copy records?

Data are not printed. In the event that it is hard copy, records are destroyed in a shredder.

Data Security

Illuminate is a web-based “all-the-data” system used by K-12 schools and districts to access student data. Teachers or administrators login to Illuminate and view student demographic and achievement data. Data is the primary element of the system and, as such, data security is paramount to Illuminate. This document will explain how Illuminate protects and values all of the data being utilized through the Illuminate systems.

Family Education Rights and Privacy Act (FERPA)
Illuminate adheres to all rules and regulations related to the protection of confidential student information as described in FERPA and District student confidentiality Board Policies. Illuminate’s extensive permissions system ensures that staff members can only access features and student records appropriate to their positions.

Permissions
Illuminate has implemented a comprehensive permission system that allows clients to establish precise access rights over software features and district data. This includes field-level permissions for sensitive data. All permissions are managed through an easy-to-use online web interface. The permission structure in Illuminate is paramount in enforcing FERPA compliance.

Password Security
We do not provide any information pertaining to admin accounts and do not provide hidden backdoors to the platform; however, Illuminate maintains a general/global administrator account as a safeguard.

Data Access
User access via the web UI
Only users who have been authorized by the school district may login to the Illuminate system. Illuminate offers third party authentication (Active Directory, Google, etc.) integration options to clients who are leveraging the tools in order to bolster login security. All authorized users are provisioned their own individual account, and must provide appropriate credentials with every login. Additionally, users are automatically logged out of the system after a period of inactivity.

Direct database access
At the client’s request, direct read-only access to the Illuminate database can be granted to specific administrative users. This read-only access provides access only to the client database. All data is transmitted via SSL. The database user is given specific credentials to login to the database and access to the database is restricted to a client-specified IP address.

API access

Illuminate offers an open API to external parties at the request of clients. Prior to establishing the API access, the external party's data usage plan is evaluated by Illuminate staff. All API consumers are vetted by Illuminate. Once an API partner has been provided secure API access, the actual access to a district's installation is controlled by the district. API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls.

SFTP file transfers

Where routine file transfers are necessary for data imports and exports, only authorized users are granted restricted access to an Illuminate SFTP server. Secure FTP is used to ensure that sensitive data is encrypted in transit.

Software Security

All Illuminate data is stored securely and encrypted during transmission. The security at the software level includes secure access to the Illuminate API, single tenancy to ensure data privacy across clients, and transport layer security.

Secure API Access

API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls. Every time data is accessed via the API, both the consumer token and the client access keys are evaluated for security.

Single Tenancy

Each district's data is stored in its own dedicated database. Data is never co-mingled with data from other Illuminate clients. File transfers are also sent to district-specific locations to ensure that districts do not have visibility into each other's data.

Transport Layer Security

All Illuminate web traffic is encrypted over the wire via SSL. Firewalls are used to limit access to only essential services. Direct database access for district technical staff is managed by Illuminate, and all database traffic is also encrypted in transit via SSL.

Data Center and Cloud Provider

Illuminate products hosted in the Google Cloud Platform benefit from the same security precautions Google uses for its own products. Physical data centers include multi-layered security featuring camera and physical monitoring, credential scanning, and biometric checks.

https://cloud.google.com/security/overview/whitepaper

Illuminate also leverages a physical data center in Los Angeles and a cloud-based data center at Amazon Web Services.

Google data center security includes:

- Key card access
- Biometric scanners
- Double mantrap entry
- 24x7x365 perimeter and interior recorded video surveillance
- 24x7x365 in-house security guards
- Locked server cabinets

Google data center certifications include:

- NIST SP 800–61
- ISO 50001

Backup and Disaster Recovery

Illuminate maintains both onsite and offsite backups for all client databases, allowing us to store and retrieve data anytime. Backups are shipped offsite nightly, and are encrypted at rest to prevent data theft. In the event of a catastrophic data center failure, we can retrieve data that is at most 24 hours old.

Audit Logs

Logging occurs at multiple levels within the system. We maintain a log in the system database that records data-changing operations. Page accesses can also optionally be recorded in a flat file showing the page accessed, the user performing the access, and the date/time of the access. Certain areas of the system, such as official student grades, also have their own logging features that track more detailed information about each transaction.

Conclusion

Illuminate believes in students and educators and takes the security of their data very seriously. Illuminate has gone to great lengths to ensure that data is secure physically, in all methods of data transit, and via the software application. Additionally, all Illuminate staff is trained on FERPA and the severe importance of data security. Users of the Illuminate system can use the system confidently, knowing that Illuminate deeply values data security.