

Vendor Statement of Compliance for Data Privacy and Protection

This agreement is entered into between Roseville City School District (“LEA”) and McGraw-Hill Education (“Service Provider”) on Tuesday, January 5, 2016 (“Effective Date”).

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services titled ELA Curriculum K-5 Pilot and 6-8 StudySync Pilot (“Educational Technology Services Agreement”);

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)

- 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
- 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
- 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



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 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 6 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., **and upon district request.**
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.
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 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

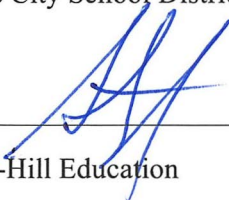
As an authorized representative of my organization, I accept the conditions listed in this document.



1/15/2016

Roseville City School District

Date



1/14/2016

McGraw-Hill Education

Date

Exhibits

Section I.6 External Security:

See attached document

Section I.7 Internal Security:

See attached document

Section II.2 Exporting of student created content:

See attached document

Section II.4 Review and correcting personally identifiable information:

See attached document

Section II.5 Securing student data:

See attached document

Section II.6 Disclosure notification:

See attached document

Section II.8 FERPA compliance:

See attached document

Section III.5 How student data is protected:

See attached document

Roseville City School District
Vendor Statement of Compliance for Data Privacy and Protection Exhibits

Section 1.6 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.

Our applications have multiple layers of network security. Each layer has its own firewalls. Additional security controls include load balancers and intrusion detection devices.

McGraw-Hill incorporates a Tier 3 design and resilient systems to support The McGraw-Hill Companies mission critical applications.

The McGraw-Hill Network infrastructure offers:

- Multiple, monitored firewalls
- Intrusion detection systems
- Intrusion prevention systems
- Redundant and diverse Internet connectivity to Gigabit speeds.
- Redundant switch fabric to the server level

DISTRICT ACCESS:

Vendor must provide a secure means (see Item 6 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).

Web application transfers data using http and https protocols. Also encryption, hashing and authorization happens to secure the data transfer. All of the reports can be exported as an Excel or .CSV file and then imported into Performance Plus.

Section 1.7 Internal Security:

Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks.

McGraw-Hill servers are behind secure multi-level firewalls with state of the art intrusion security software that minimizes the risk of malicious attacks, intrusions or hacking into the system. McGraw-Hill also does twice a year security scans, both at the application and data center level to ensure the highest level of security for our customers.

Describe the interactions vendor personal (or their representatives) will have directly with District data.

McGraw-Hill Higher Education does not share any assignment or test scores with any outside parties or affiliates.

How is uploaded data from the District handled and processed?

Data is separated logically based on purchasing account information in our database. Data in transit is protected by hashing, AES encryption and Secure Socket Layer (SSL).

Who has access to this data?

Our datacenters are physically accessible only by authorized personnel protected by access card readers, on-site security personnel and video monitoring systems. Database access is restricted to key personnel responsible for the development of specific platform services. This practice is enforced by management.

What happens to the data after the upload is complete?

Data is maintained indefinitely in our data centers. Data can be disposed of upon written request from customers.

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

Regular log analysis is done to monitor system vulnerabilities. Regular reviews are conducted and proactive actions are taken. Assigned user accounts are used for authenticating callers. User accounts can be disabled, deleted or reset as needed. User accounts must be approved by management.

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

Our Connect backups are taken at several intervals daily, weekly, monthly and stored at our onsite locations as well as offsite locations for 12 months. The EZ-Test database is backed up incrementally daily, weekly full and saved for two weeks on site.

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

Data is saved offsite for 12 months, after that time the encrypted media is securely erased and overwritten when returned onsite.

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

McGraw-Hill Education does not print copies of our data.

Section II.2 Exporting of student created content:

Vendor must attach to this document a description of how student created content can be exported and/or transferred to a personal account.

Upon a student's request to MHE, MHE shall provide student generated content in an accessible format to such student.

Section II.4 Review and correcting personally identifiable information:

Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

The procedures by which students, parents, or legal guardians may review PII and correct erroneous information are available at: <https://www.mheducation.com/privacy.html>. If you want to review the PII you have provided or if you believe information we have is inaccurate, please contact our customer service to review or update your PII.

Phone: 800-334-7344 Fax: 800-953-8691

PreK2: seg_customerservice@mheducation.com

Section II.5 Securing student data:

Vendor will attach to this document evidence how student data is kept secure and confidential.

MHE shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of PII. MHE's security measures include the following:

- a) Access to PII is restricted solely to MHE's staff who need such access to carry out the responsibilities of MHE under the Agreement;
- b) Access to computer applications and PII are managed through appropriate user ID/password procedures;
- c) Access to PII is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such PII);
- d) Data is encrypted in transmission (including via web interface) at no less than 128-bit level encryption;
- e) MHE or an MHE authorized party performs a security scan of the application, computer systems and network housing PII using a commercially available security scanning system on an annual basis; and
- f) MHE designates and trains responsible individuals to ensure the security and confidentiality of PII.

Section II.6 Disclosure notification:

Vendor must 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.

In the event of a Security Incident, MHE shall (i) investigate the Security Incident, identify the impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to individuals (including without limitation, students, parents and legal guardians) affected by the Security Incident that MHE is required to provide, and, (iii) notify Subscriber of the Security Incident, subject to applicable confidentiality obligations and to the extent allowed and/or required by Applicable Laws.

Except to the extent prohibited by Applicable Laws, MHE shall, upon Subscriber’s written request, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

Section II.8 FERPA compliance:

Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

MHE agrees to work with Subscriber to enable compliance with the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) (“FERPA”) by maintaining policies and procedures consistent with FERPA, and by directing student, parent and legal guardian inquires to Subscriber to ensure proper authentication and FERPA compliance.

Section III.5 How student data is protected:

Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

MHE agrees that the PII is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement or the Data Security Policy, MHE shall not Process PII for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.

MHE shall maintain PII confidential, in accordance with the terms set forth in this Data Security Policy and Applicable Laws. MHE shall require all of its employees authorized by MHE to access PII and all Third Parties to comply with (i) limitations consistent with the foregoing and, (ii) all Applicable Laws.

Subscriber represents and warrants that in connection with any PII provided directly by Subscriber to MHE, Subscriber shall be solely responsible for (i) notifying End Users that MHE will Process their PII in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.



Steven R. Engel, Director, Finance
McGraw-Hill School Education

1/14/2016

Date