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 **Houghton Mifflin Harcourt (HMH)** ("Service Provider") on **January 4, 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 or 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 _____

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 _____

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.

_____ 3/11/2016

Roseville City School District Date

Nicole Genova

_____ March 11, 2016

Houghton Mifflin Harcourt 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:

HMH utilizes a depth in defense architecture for securing student data. HMH partners with Amazon Web Services (AWS) and Akamai Technologies to ensure secure communications for all of our customers. HMH utilizes firewalls, load balancing, NAT (Network Address Translation), proper key management, intrusion detection systems, monitoring and alerting, and other controls to ensure availability and confidentiality of data. Additionally, HMH hires an independent third party to test vulnerabilities in the application so as to decrease risks to the data.

Section I.7 Internal Security:

Trained HMH personnel have access to the data which has been securely transmitted to the organization. For information on how uploaded data from the District is handled and processed, please see this video http://link.brightcove.com/services/player/bcpid3186031698001?bckey=AQ~~%2cAAAC5OpoGhE~%2cW9HyF3F2n76lJzCmjTPl-kIkRCjebdoW&bctid=ref:da_userdata. Only authorized personnel have access to this data. Encryption is used to safeguard the data. Backups are GFS and databases are backed up nightly. All data is retained on-disk in AWS us-east-1 region (geographically).

Section II.2 Exporting of student created content:

Per HMH Terms of Use, the district or school owns responsibility for creating and managing student accounts while using our products for instruction. Each pupil has a personal login created as a result of this process, but their access to materials is by virtue of belonging to a class taught by district staff. Pupils do not have personal accounts in our system outside of this context, and so do not have permanent accounts to which pupil-generated content can be stored and which will persist beyond the classroom access.

Section II.4 Review and correcting personally identifiable information:

Per HMH Terms of Use, the district or school owns responsibility for any data supplied as part of the pupil's account creation or rostering process. Concerns about integrity or accuracy of that data is a matter to be resolved between the district/school and the parent/guardian/pupil.

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.5 Securing student data:

All PII at rest is encrypted using AES256. All data is encrypted in transit using TLS. Privileged access is encrypted using multi-factor VPN access (or RSA token). HMH follows the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. Employees who have access to District data do so because of their roles and responsibilities. HMH maintains all data received separate from all other data files and does not copy, reproduce or transmit data obtained except to its own agents acting for or on behalf of the District and as necessary. Transmission of data is secured by electronic systems and/or networks.

Section II.6 Disclosure notification:

Data Breach Response. In the event of a security breach involving Personal Information, we will take prompt steps to mitigate the breach, evaluate and respond to the intrusion, and cooperate and assist schools and other subscribers in efforts with respect to (i) responding to the breach, including the provision of notices to data subjects; and (ii) engaging mutually agreeable auditors or examiners in connection with the security breach, subject to reasonable notice, access and confidentiality limitations.

Section II.8 FERPA compliance:

FERPA permits a school to provide educational records (including those that contain students' personal information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of "school official" by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this personal information except for purposes of providing our learning platform to the school. We comply with FERPA by relying on this form of consent.

Section III.5 How student data is protected:

All PII at rest is encrypted using AES256. All data is encrypted in transit using TLS. Privileged access is encrypted using multi-factor VPN access (or RSA token). HMH follows the principal of "Least Privileged Access" whereby those user accounts are provided the most restrictive access necessary to perform the required business function. Employees who have access to District data do so because of their roles and responsibilities. HMH maintains all data received separate from all other data files and does not copy, reproduce or transmit data obtained except to its own agents acting for or on behalf of the District and as necessary. Transmission of data is secured by electronic systems and/or networks.