RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Kelvin Education, Inc. ("Service Provider") on 2/18/2010 ("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 ( )

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Section I: General - All Data *(Continued)*

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 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, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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 ◉ 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 ○

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

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 (•) 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 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.

Baxter Mante	Laura Assem
Print Name	Print Name (Roseville City School District)
2/18/2010	2/19/2020
Signature, Date	Signature, Date (Roseville City School District)

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section 1.6: External Security

Refer to Section 10.1 of attached Privacy Policy.
We use Heroku/AWS to manage our system infrastructure and network security. Heroku/AWS provides the following built-in security:
- Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need.
- Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

For more info:
- https://www.heroku.com/policy/security
- https://aws.amazon.com/security

Section 1.7: Internal Security

Refer to Sections 5 and 10.1 of attached Privacy Policy.
District data is available only to employed personnel who require access for a valid business or educational reason. Kelvin will ensure that all employees handling district data have received training regarding data security awareness and the appropriate processing of the district data.
District data is stored at-rest with encryption. Access to the database(s) that contain district data are protected by credentials that are routinely rotated. Backups are performed programmatically within the same infrastructure and uploaded to encrypted storage. Backups are maintained for 30 days. When backups "expire", the backup file is deleted permanently.
All physical copies of printed data is shredded when we no longer have a valid business use for them.
Access to Heroku/AWS requires two-factor authentication

Section II.2: Exporting of Student-Created Content

Refer to Section 2.6 of attached Privacy Policy.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Refer to 8.1 of attached Privacy Policy

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Refer to Section 5 of attached Privacy Policy.

Section II.6: Disclosure Notification

Refer to Section 6 of attached Privacy Policy.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Refer to Sections 2.1 and 10.6 of attached Privacy Policy.

Section III.5: How Student Data is Protected:

Refer to Section 5 of attached Privacy Policy.

Reset Form

KELVIN EDUCATION, INC.

PRIVACY AND STUDENT DATA SECURITY POLICY

This Privacy and Student Data Security Policy ("Privacy Policy") is part of and incorporated into the Agreement ("Agreement") referenced in an Order Form ("Order") executed by Kelvin Education, Inc. ("Kelvin") and the customer identified in such Order ("Customer"). Except as expressly provided in the Order, the terms of this Privacy Policy supersede all contrary or conflicting terms of the Agreement. Capitalized terms used and not otherwise defined herein shall have the same meanings given those terms in the Order or Kelvin's Standard Terms and Conditions, which are part of the Agreement.

1. Definitions.

1.1. "*Aggregate Data*" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols intended to preserve the anonymity of each individual included within such data.

1.2. "*Covered Information*" means personally identifiable information or materials, in any media or format, that meets any of the following: (i) is created or provided by a student, or the student's parent or legal guardian, to an Operator in the course of the student's, parent's or legal guardian's use of the Operator's site, service, or application for K-12 school purposes; (ii) is created or provided by an employee or agent of the K-12 school, school district, local education agency, or county office of education, to an Operator; (iii) is gathered by an Operator through the operation of a site, service, or application and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, Social Security Numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information. "Covered Information does not include de-identified information, including aggregated de-identified information, used by Kelvin to improve its products and services, for adaptive learning purposes, for customizing pupil learning, for demonstrating the effectiveness of Kelvin's products and services in the marketing of such products and services, and for developing and improving Kelvin's website, services, or applications.

1.3. "*Data Security Incident*" means an event that results in or constitutes the unauthorized access, acquisition, or disclosure of Covered Information maintained by Kelvin pursuant to the terms of the Agreement. Data Security Incidents include, but are not limited to: (i) successful attempts to gain unauthorized access to a Kelvin computer or network containing Covered Information disclosed by Customer or Customer Users to Kelvin; or (ii) a material breach of the Agreement that involves the disclosure of Covered Information by Kelvin to an unauthorized third-party.

1.4. "*Destroy*" means to remove or otherwise sanitize Covered Information from Kelvin's systems, paper files, records, databases, and any other media regardless of format, so that such data is permanently irretrievable in Kelvin's normal course of business.

1.5. "*Operator"* means the operator of an internet website; online services, including cloud computing services; online applications; or mobile applications, with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.

1.6. "*Pupil-Generated Content*" means materials created by a student, including but not limited to account information that enables ongoing ownership of such content, and excluding student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

1.7. "*School Service*" means an internet website, online service, online application, or mobile application that is designed and marketed primarily for use in a preschool, elementary school, or secondary school; is used at the direction of teachers or other employees of Customer; and collects, maintains, or uses Covered Information. School Service does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to or used by a public-education entity.

1.8. "*Subcontractor*" means any third party engaged by Kelvin to store or process Covered Information in order to provide a School Service pursuant to the terms of the Agreement.

1.9. "*Targeted Advertising*" means selecting and sending advertisements to a student based on information obtained from the student's use of the School Services provided by Kelvin pursuant to the Agreement. Targeted Advertising does not include advertising to a student (i) at an online location based on the student's current visit to that location or in response to the student's request for information or feedback; and (ii) that does not rely on information obtained from the student's use over time of the School Services provided by Kelvin pursuant to the Agreement. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

2. General Provisions.

2.1. Kelvin will comply with all applicable federal and state laws and regulations concerning the privacy and data security of Covered Information, including but not limited to California Education Code § 49073.1, also known as AB 1584; the California Student Online Personal Information Protection Act, Cal. Bus. & Prof. Code § 22584 *et seq;* the California Act for Privacy Rights for California Minors in the Digital World, Cal. Bus. & Prof. Code § 22580 *et seq.;* the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. Section 6501-6502; and the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g and 34 C.F.R. Part 99; and the Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. 1232h.

2.2. Kelvin will promptly forward to the Customer's representative pursuant to the notice provisions of the Agreement any request or demand from a third party for Covered Information in the possession of Kelvin at the time the request is received.

2.3. To the extent required by applicable state or federal law, Kelvin agrees that auditors from any state, federal, or other governmental agency, as well as auditors previously designated by Customer, shall have the option to audit the privacy and data security components of Kelvin's operations with respect to the School Services provided to Customer pursuant to the Agreement. Such records pertaining to the privacy and data security components of the School Services shall be made available to auditors and the Customer when requested.

2.4. Kelvin will provide Customer notice prior to making a material change to Kelvin's online privacy notice.

2.5. Covered Information obtained by Kelvin from Customer will continue to be the property of and under the control of Customer.

2.6. Students may retain possession and control of their own Pupil-Generated Content, and may transfer their own Pupil-Generated Content to a personal account, by submitting a written request directly to Customer. Kelvin will cooperate with Customer to fulfill such requests.

3. Subcontractors.

3.1. Kelvin will not disclose Covered Information to a Subcontractor until such Subcontractor has executed an agreement requiring the Subcontractor to comply with all applicable federal and state laws concerning the privacy and data security of Covered Information and that any actions of the Subcontractor related to the processing of Covered Information do not violate the terms of this Privacy Policy.

3.2. Upon discovering an unauthorized disclosure of Covered Information in possession of Kelvin pursuant to the terms of the Agreement that has been subsequently disclosed by Kelvin to a Subcontractor for storage or processing, Kelvin will promptly notify Customer of such unauthorized disclosure.

3.3. Customer authorizes Kelvin to disclose Covered Information to those third-parties designated by Customer pursuant to a third-party access request. Customer warrants that any such designated third-parties have a legitimate educational interest in the Covered Data. Any third-party access requests received by Kelvin through the notice provisions contained within the Agreement will result in Kelvin's granting access and processing privileges for all Covered Data stored by Kelvin to the designated third-party until such time as (i) Customer provides Kelvin with written notification that

the third-party's access and processing privileges should be withdrawn ("Withdrawal Request"), or (ii) the termination of the Agreement. Upon receipt of a Withdrawal Request, Kelvin will revoke a designated third-party's access or processing privileges as indicated within two (2) business days.

4. Destruction of Covered Information.

4.1. During the term of the Agreement, if Customer requests in writing the destruction of Covered Information collected or generated pursuant to the Agreement, Kelvin will Destroy the information within thirty (30) calendar days after the date of the request unless:

a. Kelvin obtains the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian to retain such Covered Information; or

b. The student has transferred to another public education entity and the receiving public education entity has requested that Kelvin retain the Covered Information.

4.2. Upon request, Kelvin will provide written certification that, in accordance with the Agreement, Covered Information will not be retained or available to Kelvin upon completion of the terms of the Agreement. This certification may be enforced through any lawful means, including but not limited to civil action.

5. Security and Confidentiality.

5.1. Kelvin will take all legally required actions to ensure the security and confidentiality of Covered Information, including but not limited to the designation and training of responsible individuals. Kelvin will identify those employees and contractors who will have access to Covered Information and ensure that such individuals receive instructions as to compliance with the security and confidentiality requirements of this Privacy Policy with respect to Covered Information.

5.2. Covered Information will be encrypted in transmission and at rest.

5.3. Kelvin will deploy electronic security tools and technologies in providing the School Services under the Agreement.

5.4. Kelvin warrants to Customer that its administrative, physical, and electronic safeguards are no less rigorous than accepted industry practices and comport with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement.

5.5. Kelvin will perform reviews of its data security protection measures and methods no less frequently than on an annual basis.

6. Data Security Incident.

6.1. Kelvin warrants that it has established and implemented a Data Security Incident response plan outlining organizational policies and procedures for addressing a Data Security Incident. Kelvin's response plan will require prompt response for minimizing the risk of any further data loss and any negative consequences of the breach, including potential harm to affected individuals.

6.2. Kelvin will promptly notify Customer promptly after determining that a Data Security Incident has occurred.

6.3. In the event of a Data Security Incident, Kelvin will reasonably cooperate, at its own expense, with Customer in connection with the investigation of any unauthorized disclosure of Covered Information, including regulatory investigations, litigation, or other legal process resulting from Customer's efforts to protect rights relating to the use, disclosure, or maintenance of Covered Information provided to Kelvin

6.4. In the event of a Data Security Incident, Kelvin will use its best efforts to determine the cause of the Data Security Incident. Kelvin will subsequently produce a remediation plan to reduce the risk of similar incidents in the future. Upon request, Kelvin will present its analysis and remediation plan to the Customer within thirty (30) calendar days of notifying Customer of the Data Security Incident.

6.5. Kelvin will identify and maintain a designated representative for the purpose of communicating with the Customer regarding any such Data Security Incident. Kelvin will respond to any contact from the Customer regarding a Data Security Incident within one (1) business day.

7. Disallowed and Other Activities.

7.1. Kelvin will not knowingly:

a. Collect, use or share Covered Information for any purpose not specifically authorized or contemplated by the Agreement. Kelvin may use Covered Information for a purpose not specifically authorized or contemplated by the Agreement only with the written consent of Customer.

b. Use Covered Information, or disclose Covered Information to any third-party, for the purposes of Targeted Advertising to students.

c. Use Covered Information to create a personal profile of a Customer student other than for supporting the purposes authorized by Customer.

d. Sell or license Covered Information. This prohibition does not apply to the purchase, merger, or other type of acquisition of Kelvin or its subsidiaries, or any assets of Kelvin or its subsidiaries, by another entity, so long as the successor entity continues to be subject to the provisions of this Privacy Policy.

7.2. Kelvin may use Covered Information without violating the terms of this Privacy Policy provided that such use does not involve selling or using Covered Information for Targeted Advertising or creating a personal profile of the student, and the use is for one or more of the following purposes:

a. To ensure legal or regulatory compliance.

b. To take precautions against liability.

c. To respond to or to participate in the judicial process.

d. To protect the safety of users or others.

e. To investigate a matter related to public safety.

If Kelvin uses or discloses Covered Information pursuant to this Section 7.2, Kelvin shall promptly notify Customer of such use or disclosure.

7.3. Kelvin will perform current criminal conviction checks on all of its respective employees and agents having access to Covered Information provided by Customer to Kelvin pursuant to the Agreement. A criminal conviction check performed within ninety (90) calendar days prior to the date such employee or agent begins performance or obtains access to Covered Information will be deemed to be current. Kelvin will ensure that all employees and contractors handling Covered Information pursuant to the Agreement have received training regarding data security-awareness and the appropriate processing of Covered Information.

8. Transparency Requirements.

8.1. Kelvin will facilitate access to and correction of any inaccurate Covered Information in response to a request from Customer.

8.2. Kelvin acknowledges that Customer may post this Privacy Policy to the Customer's website or other publically viewable medium pursuant to state law.

9. Exclusions.

This Privacy Policy does not:

9.1. Impose a duty on a provider of an interactive computer service, as defined in 47 U.S.C § 230, to review or enforce compliance with this Privacy Policy.

9.2. Impede the ability of a student to download, export, or otherwise save or maintain his or her own Covered Information or documents.

9.3. Limit internet service providers from providing internet connectivity to public schools or to students and their families.

9.4. Prohibit Kelvin from marketing educational products directly to parents so long as the marketing does not result from the use of Covered Information obtained by Kelvin as a result of providing Services under the Agreement.

9.5. Impose a duty on a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this Privacy Policy on that software or those applications.

10. Miscellaneous

10.1. Kelvin warrants that Covered Information stored or processed in cloud-based systems is kept protected and confidential. Cloud-based systems, when employed by Kelvin, will be fully documented by Kelvin. Access to Kelvin's cloud-based systems is only permitted via restricted access, VPN, or least-privileged access lists.

10.2. This Privacy Policy does not prohibit Kelvin's use of Covered Information to:

a. Use adaptive learning or design personalized or customized education.

b. Maintain, develop, support, improve, or troubleshoot Kelvin's website, online services, online applications, or mobile applications.

10.3. Kelvin will maintain all necessary documentation to evidence its compliance with this Privacy Policy for a period of two (2) years following the expiration or termination of the Agreement.

10.4. Kelvin will carry and maintain Professional or Errors and Omissions Liability Insurance coverage at all times throughout the term of the Agreement and any subsequent transitional periods. Such policies will insure against liability arising from network security or privacy misconduct or lack of ordinary skill in providing the services under the Agreement, including but not limited to liability arising from the theft, disclosure, or improper use of or access to Covered Information.

10.5. Nothing in this Privacy Policy shall be construed to impose liability on Kelvin for content provided by any third party or the actions of Customer and its Customer Users of the Services provided by Kelvin.

10.6. Each of the Customer and Kelvin represents and warrants that it has and will continue to receive training so as to be familiar with the provisions of the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and equivalent state provisions, and each agrees that it will comply with such provisions and take all reasonable measures necessary to protect Covered Information from disclosure.