

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Project Lead The Way, Inc., ("Service Provider") on January 9, 2020 ("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

- 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

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

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 or students and/or their parents/legal guardians, and/or for purposes of implementing the PLTW End-of-Course Assessments.

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

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

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

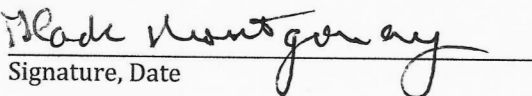
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

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


Glade T. Montgomery, Ph.D.

Print Name


Signature, Date

Laura Assem

Print Name (Roseville City School District)


Signature, Date (Roseville City School District)

EXHIBITS

Section I.6: External Security

PLTW's network is surrounded by CloudFlare's Web Application Firewall which protects against malicious activity. Additional controls include strong Access Control policies, encryption of data at rest and in transit as well as Security Event Monitoring.

Section I.7: Internal Security

Describe the interactions vendor personal (or their representatives) will have directly with District data. Limited PLTW staff have access to student data. Team Members in the IT department may have access to data for trouble shooting, Team Members in Assessments may have access to assist with Assessment related questions, and Solution Center Staff may have access to help teachers with uploads, or to troubleshoot issues.

How is uploaded data from the District handled and processed? Data uploaded from the District is transferred into PLTW databases which are encrypted. Limited staff (based on role) will have access to this data.

Who has access to this data? What happens to the data after the upload is complete? After the roster upload is completed by the District personnel, the roster file that was uploaded is deleted. The data is deleted from PLTW systems.

What security safeguards are in place to protected unauthorized access to District data? Please see the attached table of contents for the PLTW Information Security Framework for a overview of security policies.

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"?

myPLTW backups are automated and completed on a regular schedule and stored up to 2 years. Limited PLTW personnel have access to backups on a need-to-know basis. Backups are stored securely offsite in the cloud. Once the backup is expired/aged off, the data is purged and unrecoverable.

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

Section I.8: Means and Format of Extracted Data. (delimited, Excel, MDB, SQL Dump).

Vendor will provide CSV/TSV extracts of all district data.

Section II.2: Exporting of Student-Created Content

Vendor will provide CSV/TSV extracts of all data requested by a student and/or parent/legal guardian.

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

In order for a parent, legal guardian, or eligible pupil to review personally identifiable information in the pupil's records and correct erroneous information, PLTW will provide assistance through the PLTW Solution Center at 877-335-7589 or solutioncenter@pltw.org, which will provide assistance in furtherance of such requests.

Section II.5: Securing Student Data

See Table of Contents for Information Security Framework in the attached document.

Section II.6: Disclosure Notification

PLTW will notify the District who is responsible for notifying affected parties. See Table of Contents for Incident Response Policy in the attached document.

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

PLTW implements safeguards to help ensure that data remains secure and private, consistent with the following:

- (a) use or access to protected data shall be limited to PLTW representatives with a legitimate interest, including limits on internal access to education records to those individuals determined to have legitimate educational interests;
- (b) education records shall not be used for any purposes other than those explicitly authorized by the District in the Agreement;
- (c) reasonable administrative, technical and physical safeguards shall be maintained by PLTW and

its service providers and vendors to protect the security, confidentiality, and integrity of personally identifiable information in its custody, including by protecting information from unauthorized access, destruction, use, modification, or disclosure;

- (d) contracts with third party vendors and service providers that (i) require each contract to implement administrative, technical, and physical safeguards to protect personally identifiable data, (ii) include measures to be taken to address service interruptions, (iii) limit use of education records to the legitimate K-12 purposes set forth in this Agreement; and (iv) require incident response plans, breach notification and remedial measures, and liability protection and indemnification in the event of a data security incident;
- (e) encryption technology shall be used to protect data from unauthorized disclosure, and safeguards associated with industry standards and best practices, such as encryption technology, firewalls, and password protection, shall be used when data is stored or transferred;
- (f) any student records provided by the District continue to belong to and are under the control of the District;
- (g) students may retain possession and control of their own student-generated content and EOC Assessment score information and/or transfer the same to a personal account;
- (h) parents, legal guardians, or eligible students may inspect, review and correct any personally identifiable information by contacting the PLTW Solution Center team;
- (i) personally identifiable information shall not be disclosed to any party, except as follows: (a) to authorized representatives of PLTW carrying out their obligations pursuant to this Agreement, including the PLTW End-of-Course, Assessment platform provider in furtherance of District's administration of the PLTW End-of-Course Assessment; (b) to third parties where such disclosure is in furtherance of the purpose of this Agreement and such recipients are complying with legal and regulatory requirements, responding to judicial process, or otherwise protecting the safety of others or the security of the PLTW website; (c) with the prior written consent of the parent or eligible student, unless providing such notice of the disclosure is expressly prohibited by statute or court order and prior notice is instead provided to the District; or (d) to a third party entity if such information is being sold, disclosed or otherwise transferred in connection with the purchase, merger, or acquisition of PLTW by such third party entity;
- (j) personally identifiable information shall not be used for any purpose, including targeted advertising or sale or release for a commercial purpose, other than as required or specifically permitted under the Agreement between the parties and/or the Privacy Policy;
- (k) PLTW will not knowingly amass a profile about a K-12 student, except in furtherance of K-12 school purposes;

- (l) upon termination of the Agreement, PLTW will automatically initiate the removal of all nondirectory personally identifiable information provided by the District, unless otherwise required by law and except as otherwise provided in this Agreement;
- (m) appropriate and ongoing training on applicable privacy laws shall be provided to any PLTW employee and officer who will have access to such protected data; and
- (n) in the event of a data security incident which compromises personally identifiable information and that is attributable to PLTW, PLTW agrees to promptly notify the District and, to the extent agreed upon by the parties, otherwise comply with applicable laws regarding any notification obligations.

Section III.5: How Student Data is Protected:

PLTW's network is surrounded by CloudFlare's Web Application Firewall which protects against malicious activity. Additional controls include strong Access Control policies, encryption of data at rest and in transit, as well as Security Event Monitoring. Additional information is provided in the previous section.