Project Lead The Way

Educational Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

ADDENDUM

Protection of Student Personally Identifiable Information

1. **Applicability of This Addendum.**

The Wayne-Finger Lakes BOCES/EduTech and Project Lead The Way, Inc., ("PLTW"), are parties to a contract, ("Services Agreement"), signed August 8, 2022, and the relationship of the parties is fully set forth therein. The parties agree that this Addendum to the Services Agreement addresses the PLTW's protection of student personally identifiable information of PLTW Program Participant schools, as that term is defined in the Services Agreement.

2. **Definitions**

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by PLTW from PLTW's Program Participant or is created by the PLTW 's product or service in the course of being used by BOCES.

2.2. "Vendor" means Project Lead The Way, Inc., ("PLTW")_____.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by a Program Agreement from PLTW for the purpose of enabling or assisting PLTW to deliver the product or services covered by this Contract.

2.9. "The Services Agreement" means the underlying contract as modified by this Addendum.

All capitalized terms used in this Addendum or any party thereof have the same meaning in this Addendum as in the Services Agreement, unless expressed defined otherwise in the Addendum.

3. **PLTW Status**

PLTW acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. **Confidentiality of Protected Information**

PLTW agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. **PLTW Employee Training**

PLTW agrees that any of its officers or employees, who have access to Protected Information will receive training on the federal and state law governing confidentiality ofsuch information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

PLTW warrants that Protected Information received by PLTW from PLTW Program Participants or by any Assignee of PLTW, shall not be sold or used for any commercial or marketing purposes; shall not be used by PLTW or its Assignees forpurposes of receiving remuneration, directly or indirectly; shall not be used by PLTW or its Assignees for advertising purposes; shall not be used by PLTW or its Assignees to develop or improve a product or service; and shall not be used by PLTW or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by PLTW shall remain with the PLTW Program Participant, eligible student, parent, or legal guardian that provided such data.Neither PLTW nor BOCES shall acquire any ownership interest in education records or Protected Information.

7.2. Intentionally deleted by agreement of the parties. .

7.3. PLTW is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users or performing any other data analytics other than those required to provide the Product to PLTW Program Participants. PLTW is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to a PLTW Program Participant upon its request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must beperformed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which PLTW is being provided access to Protected Information is to provide the product or services that are the subject of the Program Agreement between PLTW and PLTW Program Participants.

9. Downstream Protections

PLTW agrees that, in the event that PLTW subcontracts with another entity in order to fulfill its obligations under the Program Agreement, including the purchase, lease, or sharing of server space owned by anotherentity, that entity shall be deemed to be an "Assignee" of PLTW for purposes of Education Law Section 2-d, andPLTW will only share Protected Information with such entities if those entities are contractually bound to observe obligations to maintain the privacy and security of Protected Information that are consistent with those as are required of PLTW under the Program Agreements entered into between PLTW and PLTW Program Participants and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of the Services Agreement is defined by the underlying contract.

10.2. Intentionally deleted by agreement of the parties. .

10.3. Intentionally deleted by agreement of the parties..

10.4. Intentionally deleted by agreement of the parties..

10.5. Intentionally deleted by agreement of the parties..

10.6. Intentionally deleted by agreement of the parties..

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures established between PLTW and PLTW Program Participants for amendment of education recordsunder the Family Educational Rights and Privacy Act (FERPA).

11.2. Intentionally deleted by agreement of the parties. .

12. PLTW Data Security and Privacy Plan

12.1. PLTW agrees that for the life of the Services Contract the PLTW will maintain the administrative, technical,and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Addendum and made a part of the Services Agreement.

12.2. PLTW warrants that the conditions, measures, and practices described in the PLTW 's Data Security and PrivacyPlan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the PLTW will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy(Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under the Program Agreements with PLTW Program Participants;

12.7. demonstrate that it complies with the requirements of Section 121.3© of this Part;

12.8. specify how officers or employees of the PLTW who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality ofsuch data prior to receiving access;

12.9. specify if the PLTW will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the PLTW will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify PLTW Program Participants; and

12.11. describe whether, how, and when data will be returned to PLTW Program Participants, deleted or destroyed by the PLTW when the Program Agreements are terminated or expire.

13. Additional PLTW Responsibilities

PLTW acknowledges that under Education Law Section 2-d and related regulations it has the following obligations

with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of the P Agreement:

13.1 PLTW shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 PLTW will not use Protected Information for any purpose other than those explicitly authorized in the Program Agreements;

13.3 PLTW will not disclose any Protected Information to any party who is not an authorized representative of PLTW using the information to carry out PLTW 's obligations under this Program Agreement or to PLTW Program Participants unless (1) PLTW has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to PLTW Program Participant no later than the time of disclosure, unlesssuch notice is expressly prohibited by the statute or court order;

13.4 PLTW will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 PLTW will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 PLTW will notify the PLTW Program Participant of any breach of security resulting in an unauthorized release of student data by the PLTW or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the PLTW , the PLTW shall pay for or promptly reimburse PLTW Program Participant for the full cost incurred by PLTW Program Participant to send notifications required by Education Law Section 2-d.

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For Project Lead The Way, Inc.
	DocuSigned by: DEB53FAE8FE5486...
Date 12/13/23	Date 12/6/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the NewYork State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act(FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA,89 Washington Avenue, Albany, New York12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech

Date 12/13/23

For Project Lead The Way, Inc.

DocuSigned by:

Date 12/6/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Attachment C – PLTW 's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

Project Lead The Way, Inc., ("PLTW"), shall ensure data received pursuant to the agreement executed by and between PLTW and its Program Participants, remains secure and private consistent with the following:

1. PLTW incorporates and complies with the requirements of the BOCES's Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to PLTW's possession and use of data contemplated pursuant to the Program Agreement.

2. 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.

3. Education records shall not be used for any purposes other than those explicitly authorized by the Program Participant, as contained in the Program Agreement or this Data Security and Privacy Plan, by the person that provided the Data or consent to use the Data, such as an eligible student, parent/legal guardian, or as permitted or required by law.

4. 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; by deleting covered information upon request; and by developing contracts with third party vendors and service providers that (a) require such safeguards, (b) include measures to be taken to address service interruptions, and (c) require incident response plans, breach notification and remedial measures, and liability protection and indemnification in the event of a data security incident; and (d) store data in secure cloud data centers residing in the United States of America.

5. PLTW has adopted and utilizes technologies, safeguards and practices that, at a minimum, align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, as required by Part 121. PLTW utilizes webs application firewalls, multi-factor authentication, regular information security awareness training for all Team Members, anti-virus and security incident event monitoring, IPS and IDS, and secure data centers to help protect all data, as well as maintain a comprehensive library of internal policies surrounding protection of data. PLTW implements a robust risk management program to continually monitor and mitigate risks to PLTW and data it stores, and in the event of a data security incident which compromises personally identifiable information, including any breach of security resulting in an unauthorized release of student data by PLTW or any of its subcontractors or assignees, PLTW agrees to promptly notify the Program Participant and otherwise comply with applicable laws regarding any notification obligations. Furthermore, PLTW implements safeguards including elastic load balancing, has VPCs in place, maintains a decoupled infrastructure, and requires network facing username and passwords. Server maintenance is performed by PLTW's Infrastructure and Application Development teams, including but not limited to server patches and upgrades, which is thereafter locked down with encrypted key authentication.

6. Encryption technology, as defined in Part 121.1(i), shall be used to protect data from unauthorized disclosure, and safeguards associated with industry standards and best practices, such as encryption technology, login information transmitted over SSL, firewalls, and encrypted password protection, shall be used when data is stored or transferred; encryption, as defined in Part 121.1(i), shall also be utilized to protect personally identifiable information in PLTW's

custody while in motion and at rest. All data is encrypted at rest at a volume level by default (minimum AES 256) and in transit (minimum TLS 1.2).

7. PLTW stores all data in an encrypted format within AWS data centers in the United States of America, stored with AES-256, block-level storage encryption. Keys are managed by Amazon, and individual volume keys are stable for the lifetime of the volume. PLTW reviews external audits of AWS data centers on a regular basis to ensure AWS is maintaining compliance and security requirements.

8. Information security and compliance awareness training is delivered to all PLTW team members at time of hire and on a monthly basis thereafter in an online learning platform inclusive of federal and state laws concerning the confidentiality of student, teacher or principal data.

9. PLTW implements proactive methods for identifying security breaches including monitoring IDS/IPS for events, a SIEM for aggregating event logs, as well as training for team members to identify suspicious activity. Upon confirmation of a breach, PLTW will communicate to each effected school/district within 48 business hours via email and, where required by law, telephone.

10. **Reports and Notifications of Breach and Unauthorized Release**
    a. PLTW shall promptly notify the Program Participant of any breach or unauthorized release, as those terms are defined in Part 121, of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach. Such notice shall, at a minimum, include a telephone call and e-mail to the Program Participant's listed individuals to receive Notice under the Agreement and by overnight delivery as further outlined in Notices Paragraph below.
    b. PLTW shall cooperate with the Program Participant and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
    c. Where the breach or unauthorized release of personally identifiable information is attributable to PLTW, PLTW shall pay for or promptly reimburse the Program Participant for the full cost of such notification.

11. Any Data or other student records continue to belong to the Program Participant, or to the party who provided such Data or consent to use such Data.

12. Students can retain possession and control of their own student-generated content, and possession of EOC Assessment score reports, or transfer the same to a personal account.

13. Parents, legal guardians, or eligible students may challenge the accuracy of the student data collected by notifying the District in writing, consistent with its student records policy; and PLTW agrees to abide by the District's decision to the extent a change is required.

14. 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 the Agreement; (b) to third parties where such disclosure is in furtherance of the purpose of the Program 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 Program Participant; (d) to a third party if such information is being sold, disclosed or otherwise transferred in connection with the purchase, merger, or acquisition of PLTW by such third party; (e) as otherwise permitted or required by law. PLTW shall abide by all other disclosure mandates of law, including, but not limited to, FERPA.

15. Personally identifiable information shall not be used for targeted advertising or sale or release for a commercial purpose, other than as required or specifically permitted under the Program Agreement, PLTW's Privacy Policy, or permitted or required by law.

16. PLTW will not knowingly amass a profile about a K-12 student, except in furtherance of K-12 school purposes.

17. Student data received by PLTW shall be confidential and maintained in accordance with federal and state law, and PLTW shall comply with the data security and privacy policy of the Program Participant.

18. Except as otherwise provided in the Program Agreement or this Data Security and Privacy Plan, PLTW shall not disclose any personally identifiable information to any other party without the prior documented consent of the parent or eligible student except for as specifically authorized under Part 121.9(5).

19. Subject to current legal requirements, PLTW shall have the right to receive and retain PLTW End-of-Course Assessment ("EOC Assessment") results and may use such data with PII removed in evaluating the EOC Assessments, the Program and the effectiveness of the Program, and/or the Participating Locations. Additionally, student performance on a PLTW EOC Assessment may provide long-term consequential benefits and value to students during their scholastic experience and following graduation or departure therefrom. PLTW will obtain specific consent from students and/or their parents/legal guardians during the EOC Assessment registration process to maintain these data.

20. PLTW may, either directly or through its contracted vendor, retain data and make such data available to the student that is the subject of the Data for purposes of seeking higher education and other opportunities. Such Data retention is subject to legal and or regulatory record retention requirements, and Data will be securely destroyed when the data is no longer needed for the purposes for which they were obtained, or transferred to the District or District's designee, according to a schedule and procedure as the parties may reasonable agree, unless consent to maintain the Data is obtained or as otherwise permitted by applicable law. At the request of the Program Participant, a copy of the data will be returned to the Program Participant prior to destruction. Such request must be made by the Program Participant by August 1st of the applicable school year, or the data will be destroyed in accordance with the Agreement. PLTW reserves the right to purge applicable Data at least annually, without further notice. PLTW further agrees to delete any covered information at the reasonable written request of Program Participant where such information remains under Program Participant's control.

21. PLTW may utilize subcontractors and will monitor any subcontractor or vendor that has access to personally identifiable information to ensure such third parties follow the obligations set forth herein. Where PLTW engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on PLTW by state and federal law and contract shall apply to the subcontractor.

22. Except as otherwise provided herein, PLTW will take reasonable steps to dispose of or de-identify all Data when it is no longer needed for the purpose for which it was obtained.
    a. Disposition will include (1) shredding of any hard copies of Data; (2) erasing; or (3) otherwise modifying the PII in any Data to make it unreadable or indecipherable.
    b. This duty to dispose does not extend to Data (1) for which PLTW has specifically obtained consent from the parent, legal guardian, and/or eligible student to keep; (2) that has been de-identified; and/or (3) that otherwise saved or maintained by a student.

23. PLTW represents and warrants that, prior to the receipt of student data, it will implement all state, federal, and local data security and privacy contract requirements and that it will continue to assess, audit, and otherwise modify its internal processes and this Data Security and Privacy Plan to ensure compliance with such requirements over the life of the Program Agreement, consistent with the Program Participant's data security and privacy policy.

24. Due to PLTW's legal obligations and/or Program or organizational changes, improvements, or developments, PLTW may modify certain terms of this Data Security and Privacy Plan from time to time upon reasonable notice to Program Participant in a form and delivery method determined by PLTW, and any such changes will continue to meet all applicable state and federal laws and regulations. Unless otherwise provided in notices of such changes, the most current terms shall apply to all information held by PLTW and to the terms and conditions under which the Program is operated.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment D

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which PLTW Program Participant "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by Project Lead the Way, Inc., ("PLTW") are limited to the purposes authorized in the contracts between PLTW and the PLTW Program Participants, as that term is defined in the Services Agreement. dated 8/09/2022 .

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: PLTW will ensure that any subcontractors, or other authorized persons or entities to whom PLTW will disclose the Confidential Data, if any, are contractually bound as set forth in Section 9 of the Addendum.

3. **CONTRACT PRACTICES**: The Services Agreement commences and expires on the dates set forth in the Services Agreement, unless earlier terminated or renewed pursuant to the terms of the Services Agreement.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, by contacting PLTW's Solution Center.

5. **SECURITY PRACTICESN**: Intentionally deleted by agreement of the parties.

6. **ENCRYPTION PRACTICES**: PLTW will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: DocuSigned by: _____ Date: 12/6/2023