

## PLTW CONTRACT ADDENDUM

Project Lead The Way, Inc., (“PLTW”), and Cayuga-Onondaga BOCES, (“Program Participant”), have entered into an agreement for the provision of PLTW programs by PLTW, (“Agreement”). This addendum, (“Addendum”), which conforms to the requirements of New York Education Law Section 2-d and its implementing regulations, shall supplement the Agreement and be incorporated therein. To the extent this Addendum conflicts with a previously signed Agreement between the parties, this Addendum shall control.

### A. PARENTS’ BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

The Cayuga-Onondaga BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the District wishes to inform the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purpose.
- 2) In accordance with FERPA, Section 2-d and Board Policy 7240 Student Records: Access and Challenge, parents have the right to inspect and review the complete contents of their child's education record.
- 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) The District has the following safeguards in place to protect student data, including personally identifiable information stored or transferred by the District.
  - a) All databases that have student information are protected by a secure password and login. These logins are monitored and kept up to date;
  - b) Student information is only accessible by those that are deemed warranted of having the information.
- 5) A complete list of all student data elements collected by the State is available for public review at: <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
- 6) Parents have the right to have complaints about possible breaches of student data addressed.

Complaints should be directed in writing to:

Brian K. Hartwell  
Cayuga-Onondaga BOCES  
1879 W Genesee St Rd,  
Auburn, New York 13021  
(315) 253-0361

or:

The Chief Privacy Officer, New York State  
Education Department  
89 Washington Avenue, Albany, New York 12234

Complaints may also be directed to the Chief Privacy Officer via email at: [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

**B. Part 121 Supplemental Information**

- 1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;**

PLTW provides transformative learning experiences for PreK-12 students and teachers across the U.S. We create an engaging, hands-on classroom environment and empower students to develop in-demand knowledge and skills they need to thrive. We also provide teachers with the training, resources, and support they need to engage students in real-world learning. PLTW collects personally identifiable information at the time of rostering for its programming and/or End-of-Course Assessments, during registration for professional development, and in furtherance of student and teacher opportunities from time to time. The data enable student and teacher access to course curriculum, professional development, resources, and the EOC Assessments, and student opportunities; allow PLTW to evaluate whether there is differential impact and/or bias based on demographic categories; ensure that we offer equitable programming; evaluate program impact and efficacy; continually improve our programs, products and services; enable user functionality within the courses; and provide accurate records for PLTW users. The data will be used for such purposes and consistent with FERPA, COPPA, PPRRA, and any other applicable state and federal regulations.

- 2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);**

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.

- 3. The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed):**

The duration of the Agreement is defined therein.

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.
- 4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;**

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.

**5. Where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and**

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.

**6. Address how the data will be protected using encryption while in motion and at rest.**

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).

**C. Data Security and Privacy Plan**

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

1. PLTW incorporates and complies with the requirements of the District’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 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 District, as contained in the Agreement or this Data Security and Privacy Plan, by the person that provided the Data or consent to use the Data, such as 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 web 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 District 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).

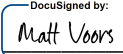
7. PLTW stores all data in an encrypted format within AWS data centers in the United States of America, stored with AES-256, block-level storage encryption. Keys are managed by Amazon, and individual volume keys are stable for the lifetime of the volume. PLTW reviews external audits of AWS data centers 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 District 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 District'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 District 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 District for the full cost of such notification.
11. Any Data or other student records continue to belong to the District, 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 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; (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 this 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 District.
18. Except as otherwise provided in the 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 District, a copy of the data will be returned to the District prior to destruction. Such request must be made by the District 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 District where such information remains under District’s control. The obligations of this agreement shall continue and shall not terminate for as long as PLTW, its employees, vendors or contractors retain PII or access to PII.
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. PLTW shall provide or require by contract appropriate training pertaining to applicable laws and regulations pertaining to the confidentiality of personally identifiable information.
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 this Agreement, consistent with the District's data security and privacy policy.

- 24. District acknowledges that, 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 District 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.

PROJECT LEAD THE WAY, INC.

By:   
SAE0995140BE4C8  
Matthew Voors  
EYP Chief Legal and Compliance Officer  
Date: 3/1/2024

CAYUGA-ONONDAGA BOCES

By:   
Name: Pamela Horton  
Title: Director of Instructional Support Services  
Date: Feb 21, 2024






# Ed Law 2D Agreement - PLTW

Final Audit Report

2024-02-21

Created:	2024-02-20
By:	Taylor Albring (talbring@caybores.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA8tNW0QJeGLUYAlvijaYRqqpwEquWz-tQ

## "Ed Law 2D Agreement - PLTW" History

-  Document created by Taylor Albring (talbring@caybores.org)  
2024-02-20 - 3:35:42 PM GMT
-  Document emailed to Pam Horton (phorton@caybores.org) for signature  
2024-02-20 - 3:36:26 PM GMT
-  Email viewed by Pam Horton (phorton@caybores.org)  
2024-02-20 - 9:37:38 PM GMT
-  Document e-signed by Pam Horton (phorton@caybores.org)  
Signature Date: 2024-02-21 - 5:20:53 PM GMT - Time Source: server
-  Agreement completed.  
2024-02-21 - 5:20:53 PM GMT