STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, MISSOURI, NEW HAMPSHIRE, OHIO RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA

MA-ME-MO-NH-OH-RI-TN-VT-VA-DPA, Modified Version 1.0

Twinsburg City School District

and

Project Lead The Way, Inc.

This Student Data Privacy Agreement ("**DPA**") is an addendum to the Service Agreement, as defined below in Exhibit C, and is entered into by and between: Twinsburg City School District, located at 11136 Ravenna Road, Twinsburg, OH 44087 USA (the "**Local Education Agency**" or "**LEA**") and Project Lead The Way, Inc., located at 5939 Castle Creek Parkway North Drive, Indianapolis, IN 46250 USA (the "**Provider**"), effective upon the date of full execution, ("Effective Date").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations.

and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses and Exhibits contained herein.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   √ If checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.

3. In the event of a conflict between the DPA Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy, the Parties agree the terms of the DPA and the Service Agreement will be reconciled to the greatest extent possible. In the event such terms cannot be reconciled, the parties agree to discuss in good faith an appropriate approach and resolution, with the understanding that the terms of this DPA will control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

   The designated representative for the Provider for this DPA is:

Name: Matthew Voors
Title: EVP, Chief Legal & Compliance Officer
Address: 5939 Castle Creek Parkway North Drive, Indianapolis, Indiana 46250
Phone: 317-669-0200
Email: mvoors@pltw.org; solutioncenter@pltw.org

The designated representative for the LEA for this DPA is:

Jennifer Farthing, Director of Curriculum and Technology
11136 Ravenna Road, Twinsburg, OH 44087
330-486-2015
jfarthing@twinsburgcsd.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Twinsburg City School District

By: Jennifer C. Farthing
Jennifer C. Farthing (Jul 23, 2025 15:33:39 EDT) Date: Jul 23, 2025

Printed Name: Jennifer Farthing Title/Position: Director of Curriculum and Technology

Project Lead The Way, Inc.

DocuSigned by:
By: Matt Voors Date: 7/23/2025
5AE0965140BE4C8...

Printed Name: Matt Voors Title/Position: Chief Legal and Compliance Officer

STANDARD CLAUSES
Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.

2. **Student Data to Be Provided**. In order to perform the Services described in **Exhibit "A"** and/or any Service Agreement, the Student Data that may be processed by Provider shall be identified in the Schedule of Data, attached hereto and incorporated herein as **Exhibit "B"**.

3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. As between Provider and LEA, all Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA, however, such controls shall not limit an eligible student, parent, or legal guardian's ability to use Student Data, except for uses such as deletion of all copies that are contrary to requirements of a public entity. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data to correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

2. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, or written consent of eligible student, parent, or legal guardian, transfer, or

provide a mechanism for the applicable party to transfer, said Student-Generated Content to a separate account created by the student. Provider shall allow for transition of an account by an eligible student, parent, or legal guardian and/or provide a mechanism for students to maintain their accounts.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors to whom it discloses personally identifiable information of students in performing functions for the Provider in order for the Provider to provide the Services outlined in Exhibit A and/or pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
   a. If in the future it is required by law, LEA shall obtain any necessary verifiable written consent from eligible students, parents, or legal guardians pertaining to student participation, to share the Student Data with Provider for operation of the Services, and use of internet resources, and shall properly implement any required filtering software or mechanisms to protect students from harmful or objectionable materials.

3. **Reasonable Precautions**. LEA shall implement reasonable physical, technical, and administrative safeguards to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A , or as consented to by an LEA, or an eligible student, parent, or legal guardian in writing, as required by applicable law.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents to whom Provider provides access to personally identifiable information of students to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement or this DPA. Provider agrees each such employee or agent is bound in confidentiality by the nature of their employment and/or contract.

4. **No Disclosure**.
   a. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data other than as directed or permitted by the LEA, this DPA, or as otherwise consented to by the LEA, eligible student, parent, or legal guardian through an agreement directly between the Provider and the student who is over eighteen (18) and/or parent/legal guardian Except as specifically stated in the separate agreement, such separate agreement does not impact the Provider's obligations to maintain and process Student Data in accordance with this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information; Student Data disclosed pursuant to a request by government agencies where such disclosure is required by law or lawfully issued subpoena or other legal process; Subprocessors performing services on behalf of the Provider pursuant to this DPA; authorized users of the Services; or disclosures otherwise required by law. Provider will not Sell Student Data to any third party.

   b. The parties acknowledge and agree that use of the internet and commercially available applications by eligible students, parents, or legal guardians that are outside the control of Provider is not subject to this DPA or Services Agreement.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and applicable law, including the following purposes: (1) conducting or assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the impact and the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or underlying Service Agreement or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA or the relationship between the parties, and receipt of a written request from the LEA, Provider shall dispose of all identifiable Student Data when they are no longer needed for the purpose for which they were disclosed, received, and/or maintained or as otherwise required by applicable law, but no more than six years after matriculation.The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed or transitioned to an account controlled

by a student, parent, or legal guardian, or which Provider has obtained consent to maintain from an eligible student, parent, or legal guardian. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. Upon written request from the LEA and provision of Exhibit D, Provider will initiate the actions set forth in Exhibit D. Notwithstanding anything to the contrary, in no event shall Provider be required to retrieve, delete, and/ or return any data, including but not limited to Student Data, that is stored on digital media and may be used for archival or backup purposes. If Student Data is restored from a back-up after a deletion request, then the Provider will destroy the Student Data within a reasonable time from restoration.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services (iv) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits; or (v) to communicate with users of the Services. Private accounts established by an eligible student, parent, or legal guardian set up are not subject to the terms of this Agreement.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the

Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the LEA affected by the data breach.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written

consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. LEA has the authority to terminate the DPA if it violates federal, state or local law to contract with the successor, after written notice of such legal determination is provided.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including

confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof. LEA affirms that it has reviewed and accepts this Agreement as a binding contract. LEA further affirms that The Education Cooperative ("TEC") is an authorized agent for purposes of negotiating and administering this Agreement and Provider may disclose information (including Confidential Information) to and discuss concerns related to this Agreement with TEC. LEA shall cause TEC to be bound by obligations of confidentiality with respect to Provider's confidential information, and shall either make Provider an intended third party beneficiary of such obligation, or shall be wholly responsible for any impermissible use or disclosure of Provider's information by TEC.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

PLTW is a nonprofit organization whose mission is to empower students to thrive in an evolving world. PLTW provides transformative learning experiences for PreK-12 students and teachers across the U.S. PLTW creates 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 has established a comprehensive experience, which consists of various distinct curricular , professional development, and training products (each a "Program" and collectively, the "Programs"), that provide students and educators access to real-world applied learning experiences, support, and resources that empower them to gain skills needed to thrive in an evolving world. The services PLTW provides its district program participants are detailed within this document as well as the applicable PLTW agreement executed by and between the parties, including access to the Program(s) to the student and teacher users of District's participating schools, including, as applicable, account protected access to Program curricula as well as access to the PLTW electronic communication network; online systematic assessments; evaluation and survey instruments; account protected curricular and assessments platforms; potential student opportunities; professional development and online training; program support; potential grant funding opportunities; and additional program participant benefits. Student information will be used for these purposes and/or as otherwise consented to electronically or in writing by an eligible student, parent, or legal guardian. Akin to other nationally recognized college and career readiness examinations, achievement on PLTW End-of-Course Assessments provides students with post-secondary education opportunities including but not limited to higher education admissions considerations, scholarships, and dual credit as well as post-secondary and/or post-collegiate employment and career opportunities, and PLTW provides services for its students associated with post-secondary opportunities. Following completion of a PLTW End-of-Course Assessment and at any time within their myPLTW accounts, an eligible student, parent or legal guardian may opt in to the use and maintenance of the student's data and assessment scores and provide electronic consent for such use and maintenance for these purposes.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Data that may be collected by PLTW
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	x
	Other application technology meta data-Please specify: Device type	x
Application Use Statistics	Meta data on user interaction with application	x
Assessment	Standardized test scores	x
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	x
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	x
	Place of Birth	
	Gender	X optional
	Ethnicity or race	X optional
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	x
	Student grade level	x
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	x
	Year of graduation	x
	Other enrollment information-Please specify: Student post graduate plans (optional)	x
	Address	X if provided

Category of Data	Elements	Data that may be collected by PLTW
Parent/Guardian Contact Information	Email	X if provided
	Phone	X if provided
Parent/Guardian ID	Parent ID number (created to link parents to students)	X if provided
Parent/Guardian Name	First and/or Last	X if provided
Schedule	Student scheduled courses	x
	Teacher names	x
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	X testing accommodations
	Specialized education services (IEP or 504)	X testing accommodations
	Living situations (homeless/foster care)	
	Other indicator information-Please specify: Student nickname	x
Student Contact Information	Address	X optional
	Email	x
	Phone	X optional
Student Identifiers	Local (School district) ID number	x
	State ID number	x
	Provider/App assigned student ID number	x
	Student app username	x
	Student app passwords	x
Student Name	First and/or Last	x
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	x
Student Survey Responses	Student responses to surveys or questionnaires	x
Student work	Student generated content; writing, pictures, etc.	x

Category of Data	Elements	Data that may be collected by PLTW
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	x
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

Category of Data	Elements	Data that may be collected by PLTW
Other	Please list each additional data element used, stored, or collected by your application: nickname	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: Provider is defined as Project Lead The Way, Inc. .

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: For the purpose of this DPA, the Service Agreement is the underlying agreement between the Provider and LEA.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data that has not been De-Identified. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who receives personally identifiable information of students from Provider to perform such services.

Subscribing LEA: An LEA that was not party to the original DPA and who accepts the General Offer of Privacy Terms set forth in Exhibit E, attached hereto and incorporated herein.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: Intentionally deleted by agreement of the parties.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[**Insert categories of data here**] student personally identifiable information

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ Following receipt of written request of deletion, identifiable Student Data shall be disposed of as soon as commercially practicable, when the data are no longer needed for the purposes which they were obtained or maintained, and following receipt of a written request of an LEA, as set forth in this DPA.

_____ By [**Insert Date**]

4. Signature

____ ___________________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ _______________

Authorized Representative of Company Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.
*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
3. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
4. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
5. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
6. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
    c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"
Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
3. Replace Article V, Section 4(1) with the following:
    a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student's family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include, to the extent known at the time:
        i. Details of the incident, including when it occurred and when it was discovered;
        ii. The type of personal information that was obtained as a result of the breach; and
        iii. The contact person for Provider who has more information about the incident.
    b. "*Breach*" shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
    c. "*Personal information*" is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
        i. Social Security Number;
        ii. Driver's license number or other unique identification number created or collected by a government body;
        iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account;
        v. Medical information; or
        vi. Health insurance information.

EXHIBIT "G"
Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.324, R.C. §§ 1349.17-19, Rule 3301-51-04;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
2. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
3. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
4. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
5. Provider will not access or monitor any of the following:

    a. Location-tracking features of a school-issued device;
    b. Audio or visual receiving, transmitting or recording features of a school-issued device;
    c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
3. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
4. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
5. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

   i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:

      1. The credit reporting agencies
      2. Remediation service providers
      3. The attorney general

   ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

   iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq*., T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq*., T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq*.;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
3. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
4. The Provider agrees that it will not collect individual student data on:
    a. Political affiliation;
    b. Religion;
    c. Voting history; and
    d. Firearms ownership

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c);

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
3. In Article V, Section 4, add: In order to ensure the LEA's ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within forty-eight (48) hours, where the Provider discovers Student Data has been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data."

2. **"**Teacher Data" is defined as at least the following:

   Social security number.
   Date of birth.
   Personal street address.
   Personal email address.
   Personal telephone number
   Performance evaluations.

   Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

3. Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

4. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.

5. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…".

6. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

7. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

8. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17)Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18)Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19)Protect the confidentiality of Student Data and Teacher Data at rest;

(20)Identify, report, and correct system flaws in a timely manner;

(21)Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22)Monitor system security alerts and advisories and take action in response; and

(23)Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

9. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

The estimated number of students and teachers affected by the breach, if any.

10. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.

11. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

12. Teacher Data is not subject to Articles II or IV of the DPA.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Data that may be collected by PLTW
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	X
Demographics	Date of Birth	X if provided
	Place of Birth	
	Social Security Number	
	Ethnicity or race	X if provided
	Other demographic information-Please specify: gender	X if provided
Personal Contact Information	Personal Address	X if provided
	Personal Email	x
	Personal Phone	X if provided
Performance evaluations	Performance Evaluation Information	X PLTW Core Training
Schedule	Teacher scheduled courses	x
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	X Core Training
Teacher Survey Responses	Teacher responses to surveys or questionnaires	x
Teacher work	Teacher generated content; writing, pictures etc.	X
	Other teacher work data -Please specify:	X Core Training
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application Teacher first and last name Teacher Core Training information Teacher PLTW course schedule	x

PLTW_SDPA clean_final (TEC) - Twinsburg CSD, VendorSigned

Final Audit Report 2025-07-23

Created:	2025-07-23
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAQchuJgiataqwqJJofwbJJm-iJd_6WjRz

"PLTW_SDPA clean_final (TEC) - Twinsburg CSD, VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2025-07-23 - 7:26:28 PM GMT

Document emailed to jfarthing@twinsburgcsd.org for signature
2025-07-23 - 7:26:34 PM GMT

Email viewed by jfarthing@twinsburgcsd.org
2025-07-23 - 7:32:50 PM GMT

Signer jfarthing@twinsburgcsd.org entered name at signing as Jennifer C. Farthing
2025-07-23 - 7:33:37 PM GMT

Document e-signed by Jennifer C. Farthing (jfarthing@twinsburgcsd.org)
Signature Date: 2025-07-23 - 7:33:39 PM GMT - Time Source: server

Agreement completed.
2025-07-23 - 7:33:39 PM GMT