

# **STANDARD STUDENT DATA PRIVACY AGREEMENT**

**WA-NDPA Standard**

**Version 1.0**

**Local Education Agency (LEA):**

Lake Washington School District

**and**

**Provider:**

Project Lead The Way, Inc.

**DATE:**

*3/25/2022*

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

School District: Lake Washington School District , located at: 16250 NE 74th Street, Redmond, WA 98052 (“**LEA**”) and  
Provider: Project Lead The Way, Inc. , located at: 5939 Castle Creek Parkway North Drive, Indianapolis, Indiana 46250 (the “**Provider**”).

**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 Privacy 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 hereto.
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, LEA and Provider agree to the additional terms of modifications set forth in **Exhibit “H”**
  - 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 SDPC 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 terms of this DPA shall control.
4. [Reserved]
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: Matt Voors Title: EVP and Chief Legal and Compliance Officer

Address: 5939 Castle Creek Parkway North Drive, Indianapolis, Indiana 46250

Phone: 877-335-7589 Email: mvoors@pltw.org; legal@pltw.org

The designated representative for the LEA for this DPA is:


Name: Donneta Oremus Title: Director of College & Career Readiness

Address: 16250 NE 74th Street, Redmond, WA 98052

Phone: 425.936.1387 Email: doremus@lwsd.org

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

**LEA:** Lake Washington School District

By:  Donneta Oremus (Mar 28, 2022 13:11 PDT) Date: 03/28/22

Printed Name: Donneta Oremus Title/Position: Director of College & Career Readiness

**Name of Provider:** Project Lead The Way, Inc.

By:  Matt Voors (May 18, 2022 15:34 EDT) Date: 3/25/2022

Printed Name: Matt Voors Title/Position: EVP and 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 above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto 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**. 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. 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 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.
3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
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 performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than 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.
3. **Reasonable Precautions**. LEA shall take reasonable precautions 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 stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. [See Modification at Exhibit "G"]
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on

behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

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 the following purposes: (1) 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 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 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, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
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 or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. [See modification at Exhibit "G"]

## **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 set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. 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 reporting LEA subject to this section.
    - 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 the LEA Party seeks to terminate this DPA, they are able to terminate this DPA at any time with given notice to the vendor. 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. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. 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. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
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.
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 indemand 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 education program, (the "Program"), which consists of various distinct curricular programs including PLTW Launch, PLTW Gateway, PLTW Biomedical Science, PLTW Computer Science, and PLTW Engineering and provides services related to and in furtherance of implementation of the Program. The services PLTW provides is district program participants are detailed within this document as well as the applicable PLTW agreement executed by and between the parties. PLTW will provide access to the Program to the student and teacher users of District's participating schools, including, as applicable, account protected access to Program curricula and updates as well as access to the PLTW electronic communication network; online systematic assessments; evaluation and survey instruments; potential student opportunities; professional development and online training; program support; potential grant funding opportunities; and additional program participant benefits. Akin to other nationally recognized college and career readiness examinations, achievement on PLTW EOC 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. During the EOC Assessments registration process, eligible students and/or their parents/legal guardians provide specific consent for the use and maintenance of their data for these purposes, during their completion of PLTW high school courses and following graduation therefrom.

**EXHIBIT "B"**

**SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify: <b>device type</b>	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input checked="" type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input checked="" type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input checked="" type="checkbox"/>
	Year of graduation	<input checked="" type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input checked="" type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low-income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input checked="" type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input checked="" type="checkbox"/>
	Student course grades/ performance scores	<input checked="" type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Students pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

## 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:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**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:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**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. 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 has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**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:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

District or LEA: Lake Washington School District 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:

Categories of data: **Data shall be de-identified.**

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:

Special instructions:


3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By Date: within 30 days of written req

4. Signature

  
\_\_\_\_\_  
Douglas Oremus (Mar 28, 2022 13:11 PDT)

Authorized Representative of LEA

03-28-22  
\_\_\_\_\_

Date

5. Verification of Disposition of Data

  
\_\_\_\_\_  
Douglas Oremus (Mar 28, 2022 13:11 PDT)

Authorized Representative of Company

\_\_\_\_\_

Date



**EXHIBIT "E"**

**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Lake Washington School District ("Originating LEA") which is dated 2/25/2021, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material changes in the applicable privacy statutes; (2) a material changes in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:  
dpo@pltw.org

Name of Provider: **Project Lead The Way, Inc.**

BY: Matt Voors Date: 3/25/2022  
Matt Voors (Mon 18, 2022 15:34 EDT)

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

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between originating LEA: Lake Washington School District and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

Name of Subscribing LEA: **Donneta Oremus**

By: \_\_\_\_\_ Date: 03-28-22

Printed Name: Donneta Oremus Title/Position: Director, College and Career Readiness

SCHOOL DISTRICT NAME: Lake Washington School District

DESIGNATED REPRESENTATIVE OF LEA:

Name: Pam Brown, Royce Badley

Title: Administrative Assistant, CTE Instructional Specialist

Address: 16250 NE 74th St Redmond WA 98052

Telephone Number: 425-936-1387

Email: pbrown@lwsd.org rbadley@lwsd.org

## EXHIBIT "F"

### DATA SECURITY REQUIREMENTS

#### Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider.

#### Cybersecurity Frameworks

<input type="checkbox"/>	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input checked="" type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	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.

Subprocessors - Salesforce/Heroku, AWS, SnowFlake, University of Kansas/Kite, Okta

**EXHIBIT "G" – Supplemental SDPC State Terms for [State]**

Version 1.0

1. Recitals shall have the following sections added: This Amendment for SDPC State Terms for Washington ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

School District: Lake Washington School District , located at: 16250 NE 74th Street, Redmond, WA 98052 (the "**LEA**") and  
Provider Name: Project Lead The Way, Inc. , located at: 5939 Castle Creek Parkway North Drive, Indianapolis, Indiana 46250 (the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

**WHEREAS**, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

**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 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws;

**WHEREAS**, the Provider will provide the services to LEA within the State of Washington and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable Washington laws and regulations, such as the Student User Privacy in Education Rights 28.A.604 et seq. and RCW 42.56.590; and other applicable state privacy laws and regulations; and

**WHEREAS**, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable Washington state laws and regulations.

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

1. **Term**. The term of this Amendment shall expire on the same date as the DPA.
2. **Modification to Article IV, Section 2 of the DPA**. Article 4, Section 2 of the DPA is hereby amended to read as follows:

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 stated in the Service Agreement, or authorized under the statutes referred to herein by this DPA. Provider may use or disclose data to:

- (a) Protect the security or integrity of its website, mobile application or online service.
- (b) Ensure legal or regulatory compliance or to take precautions against liability.
- (c) Respond to or participate in the judicial process.
- (d) Protect the safety of users or others on the website, mobile application or online service.
- (e) Investigate a matter related to public safety.

In undertaking the activities specified in subsections (a) through (e) above, Provider shall adhere to all applicable data protections contained in this DPA, as well as Federal and Washington State law.

3. **Modification to Article IV, Section 7 of the DPA**, Article IV, section 7 is hereby amended to add the following language:

(iv) providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part or other consideration from a third party.

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

**LEA: Lake Washington School District**

By:  Donneta Oremus (Mar 28, 2022 13:11 PDT) Date: 03/28/22

Printed Name: Donneta Oremus Title/Position: Director of College & Career Readiness

**Provider: Project Lead The Way, Inc.**

By:  Matt Voors (May 18, 2022 15:34 EDT) Date: 3/25/2022

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

**EXHIBIT "H"**  
**ADDITIONAL TERMS OR MODIFICATIONS**

The LEA and the Provider agree to the following additional terms and/or modifications. The following sections shall be modified as indicated and set forth below:

**AGREEMENT**

**Article I, Section 2**

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

**Article IV, Section 3:**

**Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees ~~to require and maintain an appropriate confidentiality agreement from~~ each employee or agent with access to Student Data is bound by the nature of their employment and/or contract to keep confidential all Student Data. ~~pursuant to the Service Agreement~~

**Article IV, Section 4.**

**No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA or as otherwise consented to by the LEA, eligible student, parent, or legal guardian. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

**Article IV, Section 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 the following purposes: (1) 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 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 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.~~

#### **Article IV, Section 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, if no written request from the LEA is received, Provider shall dispose of all Student Data when the Student Data is no longer needed for the purpose for which it was disclosed, received, and/or maintained. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified, ~~or~~ placed in a separate student account pursuant to section II 3, 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. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."

**Modification to Article V, Section 4 of the DPA,** Article V, section 4 is hereby amended to add the following language:

- (4) Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. ~~If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.~~

**Modification to Article V, Section 4 of the DPA,** Article V, section 4 is hereby amended to add the following language:

- (6) Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:
  - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
  - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
- d. Providing any other notifications or fulfilling any other requirements adopted by the Washington State Board of Education or under other State or federal laws.

**Modification to Article V, Section 5 of the DPA**, Article V, section 5 is hereby amended to add the following language:

**Subprocessors** - All Subprocessors used by the Operator-Provider to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as consistent with or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator-Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA.

**Modification to Article VII, Section 1 of the DPA**, Article V, Section 1 is hereby amended:

1. **Term and Termination**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for a period of three (3) years, or so long as the Provider performs services under this Agreement, whichever shall be longer. 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.

#### **Article VII, Section 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.~~

**Modification to Article VII of the DPA**, Article V is hereby amended to include:

10. **Select Termination of Access**. The LEA may at its sole discretion disqualify at any time any person, entity or Subprocessor authorized to access the LEA's Data by or pursuant to this DPA. Notice of disqualification shall be in writing and shall terminate a disqualified person's or entity's access to any information provided by the LEA pursuant to this DPA immediately upon delivery of the notice to the office of the Provider. Disqualification of one or more persons or entities by the LEA does not affect other persons or entities authorized by or pursuant to this DPA.

**Modification to Exhibit B of the DPA**, Exhibit B is hereby amended to add the following language:

1. Provider will check only the data required for provision of service. Optional data will not be checked.

**Modification to Exhibit C of the DPA**, Exhibit C is hereby amended to add the following definitions:

**Metadata:** .... Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator (*e.g.*, state, county) and other descriptors.

**NIST:** Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

**Persistent Unique Identifiers:** A long-lasting identification for digital objects, which allows for those digital objects to be located even if they are moved or removed.

## **EXHIBIT C – DEFINITIONS**

**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. 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~~ include De-identified Data, that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services or data that an eligible student, parent, or legal guardian provides and/or directs Provider to use for a purpose that may fall outside a K through 12 school purpose.












# WA Lake Washington 3-25-22

Final Audit Report

2022-05-18

Created:	2022-03-28
By:	Amy Holliday (aholliday@lwsd.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAILaachjGCnz_TdRr2W36EqDi9NylwZpc

## "WA Lake Washington 3-25-22" History

-  Document created by Amy Holliday (aholliday@lwsd.org)  
2022-03-28 - 6:09:23 PM GMT- IP address: 168.99.199.15
-  Document emailed to Donneta Oremus (doremus@lwsd.org) for signature  
2022-03-28 - 6:16:04 PM GMT
-  Email viewed by Donneta Oremus (doremus@lwsd.org)  
2022-03-28 - 8:02:39 PM GMT- IP address: 104.47.56.126
-  Document e-signed by Donneta Oremus (doremus@lwsd.org)  
Signature Date: 2022-03-28 - 8:11:43 PM GMT - Time Source: server- IP address: 73.53.26.77
-  Document emailed to Matt Voors (mvoors@pltw.org) for signature  
2022-03-28 - 8:11:46 PM GMT
-  Email viewed by Matt Voors (mvoors@pltw.org)  
2022-03-28 - 8:11:50 PM GMT- IP address: 52.206.70.14
-  Email viewed by Matt Voors (mvoors@pltw.org)  
2022-05-18 - 6:43:57 PM GMT- IP address: 52.206.70.14
-  Document e-signed by Matt Voors (mvoors@pltw.org)  
Signature Date: 2022-05-18 - 7:34:15 PM GMT - Time Source: server- IP address: 64.255.246.100
-  Agreement completed.  
2022-05-18 - 7:34:15 PM GMT