WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Monroe School District

AGENCY

and

Pearson Education, Inc.

on

10/5/20

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the **Monroe School District** (hereinafter referred to as "LEA") and **Pearson Education, Inc.** (hereinafter referred to as "Provider" on _____.

The parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as set forth on Exhibit "A" attached hereto; and

WHEREAS, in order to provide the Services, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. § 1232h; and

WHEREAS, the documents and data transferred from LEA and created by the Provider's Services are also subject to several Washington State privacy laws, including Student User Privacy in Education Rights ("SUPER") 28A.604.010 *et seq.*, as well as RCW 19.255.010 *et seq.* and RCW 42.56.590.

WHEREAS, for the purposes of this DPA, Provider is a School Official with legitimate educational interests in accessing educational records and performing the Services ; and

WHEREAS, the Parties wish to enter into this DPA to ensure conformity with the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Washington the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

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

LEA acknowledges that Savvas Learning Company LLC ("Savvas") is the exclusive sales agent in the K-12 market for certain products owned by Provider. Provider products covered under this DPA are designated in the list set forth on Exhibit B attached to and incorporated into this DPA by reference. To the extent that such products offer a digital, hosted component, these services are administered through Provider and as such, the data privacy and security obligations with regard to any such products covered under this DPA reside with Provider. All other matters related to purchase or ordering reside with Savvas.

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 as defined in Exhibit "C" attached hereto, transmitted to Provider from the LEA in connection with the Services provided hereunder, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SUPER and other applicable Washington State laws, 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. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.
2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational products and Services described below and as may be further outlined in Exhibit "A" attached hereto:

   The product used will be on the My Lab and Mastering platform.

3. **Student Data to Be Provided**. In order to perform the Services described herein, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached

hereto as Exhibit "B":

Enter Categories of Student Data

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C" attached hereto.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider in connection with the Services provided hereunder 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. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data 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 LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer student-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the student's records, 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 timely manner (and no later than 45 days from the date of the request to the LEA's request for Student Data in a student's records held by the Provider for the LEA 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 as part of the Services described in Exhibit "A", Provider shall, at the written request of the LEA, transfer said Student Generated Content to a separate student account upon termination of the Services described herein; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Services.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the Student Data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **Subprocessors**. Provider shall ensure all Subprocessors performing functions in connection with the Services provided hereunder, agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance** LEA shall provide Student Data to Provider for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 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 its computer systems, Services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected 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 state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SUPER and all other Washington privacy statutes.

2. **Authorized Use**. The Student Data shared in connection with the Services provided hereunder, including Persistent Unique Identifiers, shall be used for no purpose other than providing the Services and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents (including, but not limited to, Subprocessors) who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared hereunder.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, Services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and 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 LEA, which has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained hereunder, except as necessary to fulfill its provision of Services.

5. **Disposal of Data**. Upon written request, Provider shall dispose of or delete all Student Data obtained hereunder when it is no longer needed for the purpose for which it was obtained. Disposal shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable and/or indecipherable by human or digital means. Nothing herein authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposal. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D"). Upon receipt of a request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data within fifteen (15) calendar days following receipt of said request.

    a. **Partial Disposal.** LEA may request in writing a partial disposal of Student Data obtained hereunder that is no longer needed. Partial disposal of Student Data shall be subject to LEA's request to transfer Student Data to a Student Generated Content account pursuant to Article II, section 3, above.

    b. **Complete Disposal Upon Termination of the Services.** Upon termination of the Services, Provider shall dispose of or delete all Student Data obtained in connection with the Services. Prior to disposal of the data, Provider shall notify LEA of its option to transfer data to a Student Generated Content account pursuant to Article II, section 3, above, or to other accounts as may be designated by the LEA. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

    c. **Pre-termination Data Disposal Meeting.** In addition to the foregoing requirements, the LEA may request in writing that Provider participate in a meeting to discuss disposal of the Student Data prior to termination of the Service Agreement.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing,

advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or Services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" attached hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors and/or Subprocessors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

    b. **Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, according to the procedure identified in Article IV, section 5, above. Nothing herein authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposal work authorized hereunder.

    c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the provision of the Services in a secure digital environment and not copy, reproduce, or transmit Student Data obtained hereunder, except as necessary to fulfill the purpose of data requests by LEA.

    d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or who are authorized to access the Provider's computer systems and/or the Student Data. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

    e. **Security Technology**. When the Student Data is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host Student Data in an environment using a firewall that is updated according to industry standards.

    f. **Security Coordinator**. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's

Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subprocessors Bound**. Provider shall ensure Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically (no less than annual) conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

I. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. In the event that the term of the provision of the Services is anticipated to be longer than two (2) years, upon LEA's written request, Provider shall provide written confirmation to the LEA that a third party has conducted a risk assessment analysis of Provider's computer systems at some point during the period that the Services are being provided hereunder.

j. **Compliance Audit.** LEA shall have the right but shall be under no obligation to conduct audit(s), from time to time but not more than once every twelve (12) months, of Provider's records concerning its compliance obligations as set forth in this Article V. Provider shall make a summary of such records and other documents available to LEA upon written request.

2. **Data Breach**. In the event that Student Data entrusted to Provider in connection with the Services is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA in most expedient time possible, without unreasonable delay following discovery of the incident. Provider shall follow the following process:

   a. The security breach notification shall be written in plain language, shall have a title clearly indicating a Data Breach, include a summary of breach and affected data, and include steps the provider is taking toward a resolution of the breach, and shall comply with the legal or regulatory requirements applicable to the Vendor. Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, to the extent known the following information:

- **i.** The name and contact information of the reporting Provider subject to this section.
- **ii.** A list of the types of Student Data 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 and the law enforcement agency determined that notification would impede a criminal investigation.
- **v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

- **i.** Information about what the Provider has done to protect individuals whose information has been breached.
- **ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable state and federal law 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.

e. 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 copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA requests Provider's assistance providing a legally required 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.

g. 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 – INDEMNITY

Indemnity. Provider shall defend, indemnify and hold harmless the LEA, its officers, directors, employees, agents and assigns (the "Indemnitees") from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance carrier, arising out of or resulting from any third-party claim against the Indemnitees arising out of or resulting a breach of Student Data resulting from Provider's failure to comply with any of its obligations under this DPA, provided that, (a) the breach was not caused by LEA or its student users, (b) LEA provides Provider with prompt notice of any such third-party claims, liabilities, losses or causes of actions, (c) Provider is afforded the opportunity to control the defense and the settlement of the same, and (d) LEA provides reasonable assistance and cooperation to Provider in defending against and resolving any such claim. Provider's duty to defend and indemnify the LEA includes any and all claims and causes of action whether based in tort, contract, statute, or equity.
Provider's defense and indemnity obligations herein are intended to provide for the broadest indemnity rights available under Washington law and shall survive the termination of this DPA.

ARTICLE VII- GENERAL OFFER OF PRIVACY 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 this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VIII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the provision of Services hereunder. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA so long as the Provider performs services under this DPA.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent. LEA shall have the right to terminate the DPA in the event of a material breach by Provider, its employees, or agents of the terms of this DPA.

3. **Effect of Termination Survival**. If the Services are terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this DPA is:

Name: Niall Trimble
Title: Director of Curriculum & Assessment

Contact Information:
trimblen@monroe.wednet.edu
(360) 804-2574
14692 179th Ave. SE, Monroe, WA 98272

The designated representative for the Provider for this DPA is:

Name: Matt Stricker
Title: Vice President, Sales and Shared Operations
Contact Information:
Savvas Learning Company LLC
3075 W. Ray Road, Suite 200
Chandler, AZ 85226

With a copy to:

Savvas Learning Company LLC
Attn: Data Privacy Counsel
3075 W. Ray Road, Suite 200
Chandler, AZ 85226

b. Notification of Acceptance of General Offer of Terms. Not applicable

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: N/A_____
Title: _____

Contact Information:

_____
_____
_____

6. **Entire Agreement**. This DPA constitutes 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.

7. **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.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WASHINGTON, 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 IN WHICH THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Successors Bound**. This DPA is and shall be binding upon Provider's respective successors in interest 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.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Washington Student Data Privacy Agreement as of the last day noted below.

Name of Provider Pearson Education, Inc.

BY Robert Klein Robert Klein (Oct 5, 2020 09:04 EDT) Date: 10/05/2020

Printed Name: Robert Klein Title/Position: Finance Director

Address for Notice Purposes:

NT 10/7/20

Name of Local Education Agency Monroe School District

BY: Brenda Hunt Date: 10/7/2020

Printed Name: Brenda Hunt Title/Position: Chief Financial Officer

Address for Notice Purposes:

Note: In light of COVID-19 circumstances, electronic signatures will be permitted to finalize this agreement between both parties.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE. SOME COMMON EXAMPLES INCLUDE TEACHER ASSESSMENT TOOL, CLASSROOM MANAGEMENT, INTERACTIVE EDUCATIONAL GAMES, INTERACTIVE LESSON PLANNING, CLASSROOM MESSAGING APP, INTERACTIVE WHITEBOARD.]

Type of Product or Service	Name of Product or Service	Description of Product or Service
Example: Digital Curriculum	*1-2-3 Math Curriculum*	*Pre-made math lessons developed by subject matter experts for all school levels*
Teaching and learning platform with digital curriculum	*MyLab and Mastering Platform*	*Teaching and learning platform that facilitates delivery of pre-made chemistry content and related assignments*

EXHIBIT "B"

SCHEDULE OF DATA

See attached

Category of Data	Elements	Check if used by your system
Deomgraphics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or Race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	✓
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	✓
	Teacher names	✓

Category of Data	Elements	Check if used by your system
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	✓
	Phone	✓ optional
Student Identifiers	Local (School district) ID number	✓ optional
	State ID number	✓ optional
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓ (Enrypted, not plain text)
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓ - performance captured for assignments

Category of Data	Elements	Check if used by your system
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	✓ - optional; if instructor-created, yes, otherwise optional based on opt-in / opt-out.
Student work	Student generated content; writing, pictures etc.	✓
	Other student work data -Please specify:	Question / assessment responses and interaction with the instructor are all examples of student work types that could be used.
Transcript	Student course grades	✓ - limited to the application(s) in use
	Student course data	✓ - limited to the application(s) in use
	Student course grades/performance scores	✓ - limited to the application(s) in use
	Other transcript data -Please specify:	

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please	
Other	Please list each additional data element used, stored or collected by your application	In addition to the above, the below may be used: - Country / Location - Role within course - A security question and answer - LMS Student Identifier (if integrated) - Google Analytics information - Mobile phone number (this can be optionally added for password reset for some products) - Address (for delivery of physical products, if applicable)

No Student Data Collected at this time_____.
*Provider shall immediately notify LEA if this designation is no longer applicable.

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the States of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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 as identified by Washington Compact Provision 28A.705.0 The categories of Educational Records under Washington law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Indirect Identifiers: 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.

Operator: The term "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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Data Privacy Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

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.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or student-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in

aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of this 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 records. Within this DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this DPA, Pupil Records shall be the same as Educational Records, and Student Personal Information, all of which are deemed Student Data for the purposes of this DPA.

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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identities, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this DPA, and for the purposes of federal 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.

Student Generated Content: The term "Student Generated Content" means materials or content created by a student during and for the purpose of education 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.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information

collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

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 software, and who has access to Student Data.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

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 student records. 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 DISPOSAL OF DATA

Monroe School District (hereinafter referred to as "LEA") directs Pearson Education, Inc. (hereinafter referred to as "Provider") to dispose of data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. Unless modified by separate agreement pursuant to a pre-termination data disposal meeting as described in Article IV Section 5(c), the terms of the Disposal are set forth below:

Extent of Disposal	Disposal shall be:	____ Partial. The categories of data to be disposed of are set forth in an attachment to this Directive. ____ Complete. Disposal extends to all categories of data.
Nature of Disposal	Disposal shall be by:	____ Destruction or deletion of data. ____
Timing of Disposal	Data shall be disposed of by the following date:	____ As soon as commercially practicable Insert or attach special instructions

_____ _____
Authorized Representative of LEA Date

_____ _____
Verification of Disposal of Data Date
by Authorized Representative of Provider

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Additional requirements are not applicable