

Massachusetts and New Hampshire

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: Wilmington Public Schools (the “**Local Education Agency**” or “**LEA**”) and University of Oregon (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 documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Massachusetts and New Hampshire.

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, the parties agree as follows:

1. Provider agrees to offer the LEA all the same terms and conditions found in the **ME-RI-VT-DPA, Modified Version 1.0** Data Privacy Agreement between the Provider and Orange Southwest Supervisory District (“**Originating LEA**”) which is dated **5/3/22** (“**Originating DPA**”). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms in Exhibit “G” for Massachusetts and Exhibit “G” for New Hampshire, which are attached hereto, and will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of “**General Offer of Privacy Terms**” be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices**. All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA 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: PBISApps Support

Address: 1235 University of Oregon, Eugene, OR 97403-1235

Phone: 855-455-8194

Email: pbisappssupport@uoregon.edu

The designated representative for the LEA for this DPA is:

Kenneth Lord, Director of Technology & Digital Learning
Wilmington Public Schools
22 Carter Lane, Wilmington, MA 01887
978-694-6050 ext 6700
kenneth.lord@wpsk12.com

Wilmington Public Schools

Kenneth Lord

By: [Kenneth Lord \(Jul 6, 2023 07:23 EDT\)](#)

Date: Jul 6, 2023

Printed Name: Kenneth Lord

Title/Position: Director of Technology

University of Oregon

By: *Orca Merwin*

Date: Jul 5, 2023

Printed Name: Orca Merwin

Title/Position: Assoc. Dir. Innovation Partners

EXHIBIT "G"
Massachusetts

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

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

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

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

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

EXHIBIT "G"
New Hampshire

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

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

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

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

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

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

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

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.
6. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
- (2) Limit unsuccessful logon attempts;
- (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
- (4) Authorize wireless access prior to allowing such connections;
- (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
- (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
- (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
- (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
- (9) Enforce a minimum password complexity and change of characters when new passwords are created;
- (10) Perform maintenance on organizational systems;
- (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
- (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
- (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
- (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

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

- 7. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any. T
- 8. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 9. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

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






UO(SWIS)-Wilmington Public Schools DPA 20230613

Final Audit Report

2023-07-05

Created:	2023-07-05
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAPzLZ25n6II_DxGo5rITotjP65AncVUIa

"UO(SWIS)-Wilmington Public Schools DPA 20230613" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2023-07-05 - 10:39:40 PM GMT- IP address: 108.35.203.7
-  Document emailed to Orca Merwin (omerwin@uoregon.edu) for signature
2023-07-05 - 10:40:36 PM GMT
-  Email viewed by Orca Merwin (omerwin@uoregon.edu)
2023-07-05 - 10:41:20 PM GMT- IP address: 104.47.51.126
-  Document e-signed by Orca Merwin (omerwin@uoregon.edu)
Signature Date: 2023-07-05 - 10:41:49 PM GMT - Time Source: server- IP address: 128.223.174.203
-  Agreement completed.
2023-07-05 - 10:41:49 PM GMT







UO(SWIS)-Wilmington_VendorSigned

Final Audit Report

2023-07-06

Created:	2023-07-05
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAnKOfnDrYgSSUamCVgoNPtg5xA0FDjbr8

"UO(SWIS)-Wilmington_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2023-07-05 - 11:34:03 PM GMT- IP address: 108.35.203.7
-  Document emailed to kenneth.lord@wpsk12.com for signature
2023-07-05 - 11:34:39 PM GMT
-  Email viewed by kenneth.lord@wpsk12.com
2023-07-06 - 11:22:53 AM GMT- IP address: 72.93.229.114
-  Signer kenneth.lord@wpsk12.com entered name at signing as Kenneth Lord
2023-07-06 - 11:23:28 AM GMT- IP address: 72.93.229.114
-  Document e-signed by Kenneth Lord (kenneth.lord@wpsk12.com)
Signature Date: 2023-07-06 - 11:23:30 AM GMT - Time Source: server- IP address: 72.93.229.114
-  Agreement completed.
2023-07-06 - 11:23:30 AM GMT