

OREGON STUDENT DATA PRIVACY AGREEMENT
Version 2.0 (June 30, 2019)

Tigard-Tualatin School District

and

Hobsons

May 4, 2020

This Oregon Student Data Privacy Agreement ("DPA") is entered into by and between the Tigard-Tualatin School District (hereinafter referred to as "LEA") and Hobsons

(hereinafter referred to as "Provider") on May 4, 2020 . 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") pursuant to a contract dated May 4, 2020 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, 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 LEAs and created by the Provider's Services are also subject to several state student privacy laws, including SB 187, Oregon Student Information Protection Act ("OSIPA"), Or. Rev. Stat. § 646.607 – 646.652; Or. Rev. Stat. § 326.565, et seq. (Student Records); and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to 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" (Exhibit "E"), agree to allow other LEAs in Oregon 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:

ARTICLE I: PURPOSE AND SCOPE

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, OSIPA and other applicable Oregon 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.
- 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"

hereto:

Insert description

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”:
4. **DPA Definitions.** The definition of terms used in this DPA are found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

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 Agreement 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 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 on 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 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 Article I, section 2 and/or Exhibit “A”, Provider shall, at the request of the LEA, transfer a copy of said Student Generated Content to a separate student account upon termination of the Service Agreement if Provider offers such accounts.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited. The Provider shall not sell the Student Data, Student Generated Content and/or any portion thereof to any third party or other entity or allow any other

third party or other entity to sell the Student Data and/or any portion thereof. Provider shall not use, disclose, compile or transfer Student Data except as necessary to provide the Services, and shall not permit any third party or other entity to do the same.

5. **No Unauthorized Use.** Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records 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 data in accordance with Provider's requirements for accessing the Services.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access to Provider's systems, Services and hosted data. 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, OSIPA and all other applicable Oregon privacy statutes.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, personally identifiable meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, except in furtherance of providing the Services without the express written consent of the LEA.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

- 4. No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, demonstrating the efficacy of its products, including in its marketing materials, to customize the user experience, improvement of educational sites, services, or applications, and any other legally permissible purposes 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 that party agrees in writing not to attempt re-identification. Provider shall not copy, reproduce or transmit any Student Data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.
- 5. Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition 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 or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. In response to receipt of written request from LEA, 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 “Directive for Disposition of Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within thirty (30) calendar days of receipt of said request.

 - a. Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.
 - b. Complete Disposal Upon Termination of Service Agreement.** Within 6 months of termination of the Service Agreement or within 30 days of receipt of written request from LEA, Provider shall dispose or delete all Student Data obtained under 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, as long as such learning purposes are available for use by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards, 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” 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 or contractors 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 pass criminal background checks in compliance with state and local ordinances.
 - b. **Destruction of Data.** Data shall be destroyed and disposed as defined above in Article IV, section 5.
 - 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 data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of performing the Services or data requests by LEA.
 - d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. 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 service 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 data pursuant to the Service Agreement in an environment using a firewall that is periodically 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 enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the

terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:
- a. The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” 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, the following information:
 - i. The name and contact information of the Provider 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.
 - 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.
 - d. Provider agrees to adhere to all requirements in applicable State and in 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 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 subject to LEA's execution of a nondisclosure agreement.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible student unless expressly requested by LEA. If LEA request Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA or its employees, agents, users, students, student parent or legal guardian, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VII: MISCELLANEOUS

1. **Term**. 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.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate this DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article IV, section 5.
4. **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. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other agreement resulting from a solicitation, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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 below:

a. **Designated Representatives**

The designated representative for the **Provider** for this Agreement is:

Name: Amy Reitz
Title: Senior Vice President, Product
Email: amy.reitz@hobsons.com
Phone: 703-859-7367

The designated representative for the **LEA** for this Agreement is:

Name: David Moore
Title: CFO
Email: dmoore@ttsd.k12.or.us
Phone: 503-431-4016

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 OREGON, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE OF OREGON 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 Agreement, 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 is stored, maintained or used in any way.

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 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. Each party agrees to make this DPA part of and explicitly annotated in any agreement which forms a successor entity.

[Signature Page Follows]

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

Hobsons

BY: DocuSigned by:
Monica Morrell
8F3AD39C9594408... Date: May 4, 2020

Printed Name: Monica Morrell Title/Position: General Manager, Naviance

Address for Notice Purposes:

3033 Wilson Boulevard, Suite 500

Arlington, VA 22201

Tigard-Tualatin School District

BY: *David C Moore* Date: 5/18/2020

Printed Name: David Moore Title/Position: CFO

Address for Notice Purposes:

6960 SW Sandburg St.

Tigard, OR

97223

EXHIBIT "A"

DESCRIPTION OF SERVICES

Insert a description of products and services here. If more than one product or service is included, list each product.

Naviance

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	Y
	Other application technology meta data-Please specify:	Y
Application Use Statistics	Meta data on user interaction with application	Y
Assessment	Standardized test scores	Y
	Observation data	N/A
	Other assessment data-Please specify:	Y
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	Email sent in Naviance; journal entries to/ from students (optional)
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	Y
	Place of Birth	N/A

Category of Data	Elements	Check if used by your system
	Gender	Y (Optional)
	Ethnicity or race	Y (Optional)
	Language information (native, preferred or primary language spoken by student)	N/A
	Other demographic information-Please specify: Citizenship	Y (Optional)
Enrollment	Student school enrollment	Y
	Student grade level	Y
	Homeroom	Y
	Guidance counselor	Y
	Specific curriculum programs	Y
	Year of graduation	Y
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	Y
	Email	Y
	Phone	Y
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	Y

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	N/A
	Teacher names	Y
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts /health data	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	Y
	Email	Y
	Phone	Y
Student Identifiers	Local (School district) ID number	Y
	State ID number	
	Vendor/App assigned student ID number	Y
	Student app username	Y
	Student app passwords	Y
Student Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	Y
	Other student work data -Please specify:	Y
Transcript	Student course grades	Y
	Student course data	Y
	Student course grades/performance scores	Y
	Other transcript data -Please specify:	N/A
Transportation	Student bus assignment	N/A

Category of Data	Elements	Check if used by your system
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Other	Please list each additional data element used, stored or collected by your application	N/A

No Student Data Collected at this time_____.

* Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box if more space needed.

EXHIBIT “C”

DEFINITIONS

Covered Information: Covered Information is defined as it is in Oregon SB 187 (2015). The categories of Covered Information under Oregon law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

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. For purposes of this DPA, Educational Records are referred to as StudentData.

De-Identified Information (DII):

De-Identified Information is information from which any Personally Identifiable Information has been removed or obscured in a way that removes the risk of disclosure of the identity of the individual and information about them.

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

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall mean information that identifies a specific individual. It may 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, when 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 when it identifies an individual.

Provider: For purposes of the Service Agreement, 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 the DPA the term "Provider" includes the term “Third Party” as used in applicable state statutes.

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

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

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 LEA would otherwise use employees; and (2) Is under the direct control of the LEA 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 identifies a 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 identifiers, search activity, photos, voice recordings, or geolocation information. Student Data shall constitute Student Records for the purposes of this Agreement, and for the purposes of applicable Oregon and 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 De-Identified Information, 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 Agreement, 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 PII.

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 Agreement, 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

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

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

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

Insert special instructions

3. Timing of Disposition

Data shall be disposed of by the following date:

___ As soon as commercially practicable

___ By

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date