WASHINGTON STUDENT DATA PRIVACY AGREEMENT

Version 1.0 Amended

Northshore School District

and

Naviance, Inc.

This Washington Student Data Privacy Agreement ("DPA") is entered into by and between the Northshore School District (hereinafter referred to as "LEA") and Naviance, Inc. (hereinafter referred to as "Provider") on 9/6/19. 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 Date of Service Agreement ("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 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 Services pursuant to the Service Agreement; 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

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

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 transmitted to Provider from the LEA pursuant to the Service Agreement, 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:

   Naviance is a web and mobile-based college and career readiness platform owned and operated by Naviance, Inc. Naviance helps students explore goal setting, career interests, academic planning, and college preparation, while operating as the system of records for schools and districts. It allows schools and districts to guide student achievement around college and career readiness and assess their progress in meeting those institution goals.

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

   Minimally required information necessary to create their school account, including first and last names, ID numbers, email addresses, user names, and passwords for the school and district staff users; minimally required information about the students, used for school purposes to allow Clients to view student activity within Naviance is last name, unique ID number, gender, class year and district campus.

   Additional information Clients would like to host about their students within Naviance is included at the Clients' discretion for their internal review, analysis and reporting. This may include students' personal information and academic records, including students' first names, contact information, date of birth and other demographic information, grades, test results, and performance data. Clients may also host information about a student's parents or legal guardians, including, but not limited to names, street addresses and other contact information.

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C" attached hereto. In the event of a conflict, definitions used in this DPA shall prevail over term 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 by LEA, including any modifications or additions or any portion thereof from any source, in performance of this DPA, 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 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 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 request of the LEA, transfer 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 that is not a Subprocessor, or law enforcement or 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.

5. **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 a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance** LEA shall provide 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 and Provider's 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 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.

3. **Employee Obligation**. Provider shall require all officers, 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 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, for adaptive learning purposes and to customize the student experience and for 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 it is combined with other customers' data. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposal of Data**. Upon written request and consistent with the applicable terms in subsection a or b below, Provider shall dispose of or delete all Student Data obtained under the Service Agreement 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 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 disposal. Upon Provider's receipt of written request by 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.

    a. **Partial Disposal During Term of Service Agreement.** Throughout the term of the Service Agreement, LEA may request in writing partial disposal of Student Data obtained under the Service Agreement that is no longer needed.

    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 of 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.

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" 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 applicable 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 or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposal work authorized under the Service Agreement.

    c. **Security Protocols**. Both parties agree to maintain security protocols that meet applicable industry standards in the transfer or transmission of the Student Data, including ensuring that Student 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 Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, 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. **Mobile Use of Student Data.** Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of Student Data by Provider's employees, contractors and/or Subprocessors shall be protected by industry standard encryption to prevent unauthorized access by third parties. Provider shall also implement a Bring Your Own Device

("BYOD") policy for its own employees, which requires them to use physical and technical safeguards against third party access to the device, and a copy of that BYOD policy shall be provided to LEA as part of Exhibit F to this DPA. Provider shall ensure that all contractors and/or Subprocessors implement BYOD policies, which provide for substantially the same level of security for mobile devices as are provided by Provider's BYOD policy.

f. **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 data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

g. **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.

h. **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 (no less than semi-annually) 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 semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. In the event that the term of the Service Agreement is anticipated to be longer than two (2) years, 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 term of the Service Agreement.

j. **Compliance Audit.** Provider will provide LEA with Provider's annual SOC2 report upon LEA's written request and execution of a nondisclosure agreement.

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 and shall present the information described herein under similar 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 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. Steps that the person whose information has been breached may take to help protect himself or herself if known to the Provider.

d. Provider agrees to adhere to all applicable 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 is consistent with industry standards and federal and state law for responding to a data breach, and agrees to provide LEA, upon written request, with a copy of a summary of said written incident response plan but only upon 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 or required by law. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall provide reasonable assistance.

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 at LEA's sole expense.

ARTICLE VI: 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 the DPA and Service Agreement in accordance the terms of the Service Agreement.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student 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 applicable privacy protections, including those found in FERPA and all applicable privacy statutes. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence.

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, with the exception of notices provided in Section V (2), which shall be initially provided to the LEA business contact of record, which may be different from the contact provided below:

a. Designated Representatives

The designated representative for the LEA for this DPA is:

Name: Allen Miedema
Title: Executive Director for Technology

Contact Information:
3330 Monte Villa Parkway
Bothell, WA 98021
amiedema@nsd.org

The designated representative for the Provider for this DPA is:

Name: Monica Morrell
Title: General Manager

Contact Information:
3033 Wilson Boulevard, Suite 500
Arlington, VA 22201
monica.morrell@hobsons.com

The designated representative for the Provider is:

Name: Monica Morrell
Title: General Manager

Contact Information:
3033 Wilson Boulevard, Suite 500
Arlington, VA 22201
monica.morrell@hobsons.com

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 will enter into agreements with substantially similar terms to 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.

Naviance, Inc.

BY: Monica Morrell Date: 9/9/19

Printed Name: Monica Morrell Title/Position: General Manager

Address for Notice Purposes:
3033 Wilson Boulevard, Suite 500
Arlington, VA 22201

Northshore School District

BY: _____ Date: _____

Printed Name: Allen Miedema Title/Position: Executive Director for Technology

Address for Notice Purposes:
3330 Monte Villa Parkway
Bothell, WA 98021

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Provider has outlined the services in Article I: Purpose and Scope, "Nature of Services Provided".

Matching Features. The college planning function contained in the Service includes certain optional features (collectively, "Matching") that allow students to view information from and interact with Hobsons' higher education Intersect subscribers ("Higher Education Institutions"). Matching is inactive by default, and therefore must be enabled by an authorized representative of Customer who has obtained consent from the student's parent or legal guardian prior to the activation of Matching. Matching may be turned on or off at any time at the sole discretion and control of Customer.

If Customer enables Matching for its students, its students will be able to:

View supplemental material on college profile pages and upcoming informational and other pre-enrollment events, and RSVP to upcoming events hosted by Higher Education Institutions.

In addition, students who meet certain non-personally identifiable criteria will:

Receive additional information about nonprofit Higher Education Institutions, and if a student expresses interest in a nonprofit Higher Education Institution, that student will receive an invitation through the Service to connect directly with the Higher Education Institution. The student may then choose either to disregard or to respond to the invitation.

No student or Customer information is shared with any Higher Education Institution unless Customer has enabled Matching and the applicable student has explicitly opted to send his/her information directly to the Higher Education Institution.

EXHIBIT "B"

SCHEDULE OF DATA

Provider has outlined the services in Article I: Purpose and Scope, "Nature of Services Provided".

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	N/A
	Other assessment data-Please specify:	X
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
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	X
	Place of Birth	N/A
	Gender	X
	Ethnicity or race	X

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

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

Category of Data	Elements	Check if used by your system
	wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X student enters
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	X
	Other student work data -Please specify:	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data -Please specify:	
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	X
	Other transportation data -Please	N/A

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

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

EXHIBIT "C"

DEFINITIONS

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.705.010. 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 Vendor 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 mean information that identifies an individual. It may include, but IS 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" 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 Agreement, Pupil Records shall be the same as Educational Records, and Student Personal Information, all of which, when identifiable of an individual, 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 Agreement 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 identifies 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 Agreement, 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 and who accepts the Provider's General Offer of Privacy Terms.

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 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 Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

N/A