NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT VERSION (2019)

Fremont School District (SAU 83)

and

Blackboard Inc.

April 29, 2020

This New Hampshire Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Fremont School District ((hereinafter referred to as "LEA" or "Local Education Agency") and Blackboard Inc (hereinafter referred to as "Provider" or "Blackboard") on April 29, 2020 and forms a part of the underlying agreement (the "Master Agreement") between Provider and LEA for the purchase or renewal of one or more Services outlined in Exhibit A. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, pursuant to the agreement between Blackboard and LEA effectively dated July 19, 2018 ("Service Agreement") the Provider has agreed to provide the Local Education Agency ("LEA") with one, all, or a combination of the services ("Services") as described in Article I and Exhibit "A"; which shall also be included in the term "Service(s), and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of this DPA for the Services described, without the need to negotiate terms in a separate data privacy addendum; and

WHEREAS, in order to provide the Services described in Article 1 and Exhibit A, 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 and 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; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from New Hampshire LEAs and created by the Provider's Services are also subject to several New Hampshire student privacy laws, including, where applicable, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into this 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.

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 (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable federal and state privacy statutes, including, where applicable, FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official (as defined in Exhibit "C") with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA with respect to Provider's specific provision of Services to the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the Services to the LEA described in Exhibit "A" and as indicated in the Service Agreement.

s

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the necessary Student Data that may include the categories of Student Data described in the Schedule of Data, attached hereto as Exhibit "B".

4. **DPA Definitions**. The definitions of the 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 all other writings, including, but not limited to, the Service Agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records 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 or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, 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 and the Provider's specific provision of Services to the LEA, notwithstanding the above. The LEA may have the ability to access and make changes to Student Data directly via the application's user interface, or in the alternative LEA may make a request to the Provider for an extract of Student Data and Provider will provide Student Data, as available, within ten (10) days of the LEA's request. Provider may transfer pupil-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 PII in the Pupil's Records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. The LEA may have the ability to access and make changes to Student Data directly via the application's user interface, or in the alternative, LEA may make a request to the Provider for an extract of Student Data and Provider will provide Student Data, as available, within ten (10) days of LEA request. In the event that a parent of a pupil or other guardian contacts the Provider to review any of the Pupil Records or Student Data accessed pursuant to the Services, the Provider shall refer the parent or other guardian to the LEA in a reasonable time, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Pupil Generated Content to a separate student account. Notwithstanding the foregoing, the Services contemplated herein will not require any Pupil Generate Content, and as such, Provider shall not be required to transfer Pupil Generated Content to a separate account.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall, where legally permissible, redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. 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.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement and have access to Student Data, whereby the Subprocessors agree to protect Student Data in manner materially similar or better than as provided pursuant to the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide data for the purposes of the Services Agreement and this DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA, as applicable. LEA shall ensure that it has obtained and provided all required consents and/or disclosures to users, students, or students' parents/guardians regarding Blackboard's collection, access, and use of Student Data under the Services Agreement, including to the extent applicable, to permit Provider to college Student Data directly from students under age 13 as permitted under the Children's Online Privacy and Protections Act ("COPPA") and that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted data.

3. **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 New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as 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, any meta data, user content or other non-public information , without the express written consent of the LEA or as otherwise permitted by this DPA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

   In addition, and notwithstanding any of the forgoing, provided that the Provider Processes only the minimum amount of Personal Information necessary, and the output of the Processing is aggregated or De-identified Data, LEA agrees Provider may also Process Personal Information as necessary to enforce its rights under the Services Agreement.

   LEA acknowledges that where Provider Processes Personal Information: (i) in the context of a direct relationship Provider has with an Authorized User in the course of providing or offering services to them; or (ii) with the consent of an Authorized User solely with respect to their own Personal Information, Provider's Processing activities are outside the scope of this DPA. Such relationship with the Authorized user does not diminish or undermine the Provider's obligations to the LEA under this DPA. LEA agrees to Blackboard's fulfilment of any legally satisfactory request and consent by an Authorized User to download, export, save, maintain or transfer their own personal information.

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 Student Data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data.

4. **No Disclosure**. De-Identified Information, as defined in Exhibit "C", 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). The Provider and LEA agree that the Provider

cannot successfully de-identify information if there are only a small sample of students in a particular field or category of information collected, i.e., a small sample of students in a particular grade, a small sample of students of a particular race, or a small sample of students with a particular disability. The Provider may use and transfer the De-Identified Information to a third party to help the Provider conduct its own research projects or to develop and improve the Provider's services, if the third-party agrees to not re-identify the data in writing. Otherwise, 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 the LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any Student Data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA.

5. **Disposition of Data**. Upon request, Provider shall dispose or delete all PII obtained under the Services Agreement and this DPA when it is no longer needed for the purpose for which it was obtained and, upon LEA request, Provider shall transfer said data, as available, to LEA or LEA's designee according to a schedule and procedure as the Parties may reasonably agree. Nothing in this DPA authorizes Provider to maintain PII obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Upon written request by the LEA, Provider shall provide written notification to LEA when the PII has been disposed. The duty to dispose of PII shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of this DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D"). The LEA may have the ability to access and make changes to Student Data directly via the application's user interface, or in the alternative, LEA may make a request to the Provider for an extract of Student Data and Provider will provide Student Data, as available, within 10 days LEA request.

6. **Advertising Prohibition**. Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or 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 outlined herein or as necessary to provide the Service to 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. These measures shall include, but may not be limited to:

    a. **Passwords and Employee Access**. Provider shall make best efforts to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a

level suggested by industry standards. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Subject to applicable law, all employees hired after 1/1/2011 with access to Student Data shall pass criminal background checks.

b. Destruction of Data. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained. Upon request, Provider shall transfer said data, as available, to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. Security Protocols. Both parties agree to maintain security protocols aligned with industry standard practices 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 Service Agreement in a secure computer environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Service Agreement, except as necessary to fulfill the provisioning of the Services or the purpose of Student Data requests by LEA or as otherwise permitted by the Service Agreement. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

d. Employee Training. The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the systems that store PII. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, upon request by the LEA, Provider shall provide LEA with contact information 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, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect PII from unauthorized access. The security measures shall include server authentication and data encryption. Provider shall host PII pursuant to the Service Agreement in an environment that employs boundary protection mechanisms (e.g. firewalls) that are periodically updated according to commercially reasonable standards.

f. Security Coordinator. Upon request by the LEA, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner materially consistent with the terms of this Article V. The Provider will remain responsible for Subprocessors compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors that cause the Provider to breach any of the Provider's obligations under this DPA to the same extent Provider would be liable if performing the Services itself.

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in accordance with Provider's vulnerability management policies.

i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

j. **Audits.** No more than once a year, except in the case of a verified Data Breach (as defined below) , the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof, subject to reasonable time and manner restrictions, and subject to LEA agreeing to reasonable confidentiality restrictions. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents at Provider's principal place of business during normal business hours and LEA's Student Data and all records that directly and specifically pertain to the Provider, LEA and delivery of Services to the Provider.

k. **New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. 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 in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student 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 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.

2. **Data Breach**. In the event that Provider has knowledge or a reasonable belief that Student Data has been accessed or obtained by an unauthorized individual ("Data Breach"), Provider shall provide notification to LEA as soon as practicable and no later than within ten (10) business days of the Data Breach. Provider shall follow the following process:

   a. The Data Breach notification shall be written in plain language and shall present the information described herein as available. Additional information may be provided as a supplement to the notice.

   b. The Data Breach notification described above in section 2(a) shall include the following information as available:

      i. The name and contact information of the reporting LEA subject to this section.

      ii. A list of the types of PII that were or are reasonably believed to have been the subject of a Data Breach.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Data Breach, (2) the estimated date of the Data Breach, or (3) the date range within which the Data 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 Data Breach, if that information is possible to determine at the time the notice is provided.

      vi. The estimated number of students and teachers affected by the breach, if any.

   c. At LEA's request, the Data Breach notification to the LEA will also include the following as it becomes available:

      i. Information about what the Provider has done to protect individuals whose information has been breached.

      ii. To the extent required under New Hampshire law, advise on steps that the person whose information has been breached may take to protect himself or herself.

   d. Provider agrees to adhere to all applicable requirements in the New Hampshire Data Breach law and in federal law with respect to a Data Breach related to the PII, 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. At the request of the LEA, Provider shall reasonably assist the LEA with their legally required notifications to the affected parent, legal guardian or eligible pupil of the Data Breach, which shall include the information listed in subsections (b) and (c), above. The LEA remains ultimately responsible for the timing and content of such legally required notifications.

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 whichever is later.

2. **Termination**. Either party may seek to terminate this DPA and the Service Agreement if the other party materially breaches any terms of this DPA and fails to cure such material breach within thirty (30) days written notice of such material breach.

3. **Effect of Termination Survival**. If this DPA is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the applicable privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of this DPA and the Service Agreement, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other 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, facsimile 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.

   The designated representative for the Provider for this Agreement is:

   Blackboard Inc.
   Privacy
   11720 Plaza America Drive, 10th floor Reston, VA 20190
   1-800-424-9299
   privacy@blackboard.com

   The designated representative for the LEA for this Agreement is:

   Carla Smith, Technology Director
   carla_smith@sau83.org, 603-895-2251 x202
   Fremont School District
   432 Main Street, Fremont, NH 03044

Notification of Acceptance of General Offer of Terms. Provider may agree by signing Exhibit "E", General Offer of Terms to be bound by the terms of this DPA for the services described therein for other LEAs who wish to leverage this DPA and has agreed to Contractor's Master Services Agreement (i.e. Services Agreement) which references and incorporates this DPA.

6. **Waiver; Modification**. . 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 NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF ROCKINGHAM COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement.

10. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.

ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to a Subscribing LEA (as defined in Exhibit C). Provider shall be bound to the Subscribing LEA solely as it related to the Subscribing LEA's purchase or renewal of the Services outlined in Exhibit A and pursuant to a mutual Master Services Agreement (i.e. Services Agreement) which references and incorporates this DPA.

[*Signature Page Follows*]

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

FREMONT SCHOOL DISTRICT (SAU 83)

By: Carla L. Smith
Carla L. Smith (May 14, 2020 17:07 EDT)

Date: 5/1/2020

Printed Name: Carla Smith

Title/Position: Technology Director

BLACKBOARD INC.

By:

Date: April 29, 2020

Printed Name: Bill Jones

Title/Position: Deputy General Counsel

EXHIBIT "A"

DESCRIPTION OF SERVICES

The following is a list of Services that may be purchased or renewed pursuant to this DPA. The actual Services purchased by an LEA shall be addressed in the Agreement between LEA and Provider.

Blackboard Web Community Manager

Blackboard Web Community Manager Dashboard

Blackboard Mobile Communications App Basic

Blackboard Mobile Communications App Integrated

Blackboard Mass Notification

Blackboard Connect (select markets only)

Blackboard Teacher Communications

Blackboard Integrated Student Data

Blackboard Social Media Manager

BB Comms HQ app

Blackboard Connect App (select markets only)

My Connect

TipTxt App

Blackboard Ally

[INSERT DETAILED DESCRIPTION OF SERVICES HERE]

EXHIBIT "B"

SCHEDULE OF DATA

**Please note, the Schedule of Data contains categories of data that may be provided to use the Service(s). What is actually provided is at the discretion of the LEA.*

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: e.g.,Information captured in logs	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: e.g., Test scores and number of attempts	X
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	X
	Gender	X
	Ethnicity or race	
	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:	X

Category of Data	Elements	Check if used by your system
	e.g., Other student data elements can be made available in the WCM Dashboard (which uses BB Comms Data): Class Schedule, Attendance information, etc.	
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
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student	X

Category of Data	Elements	Check if used by your system
	ID number	
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
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: Student generated content is unlikely but possible in WCM.	X

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	X
	Student course data	X
	Student course grades/performance scores	X
	Other transcript data -Please specify:	
Transportation	Student bus assignment	X
	Student pick up and/or drop off location	X
	Student bus card ID number	X
	Other transportation data - Please specify: e.g., Other transportation related information that the client may elect to process/store.	X
Other	Please list each additional data element used, stored or collected by your application: e..g, Other student data elements can be made available in the WCM Dashboard (which uses BB Comms Data): Assignments, Grades, Lunch Balances, etc.	X

EXHIBIT "C"

DEFINITIONS

De-Identified Information (DII): The terms "De-Identified Information" or "DII" shall mean information that once included Personally Identifiable Information ("PII") but such PII has been removed or obscured by the Provider in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" mean any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to any individual and shall include, but are not limited to, Student Data and metadata 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, the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address

Unique pupil identifier
Credit card account number, insurance account number, and financial services account number
Name of the student's parents or other family members

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil 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 pupil content.

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 local educational LEA employee.

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. The definition of "school official" encompasses the definition of "authorized school personnel" under 603 CMR 23.02.

Student Data: Student Data means any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that includes PII 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, 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, student identifiers, 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 New Hampshire 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 that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subscribing LEA: means a K-12 school district or institution in the State of New Hampshire purchasing one or more of the Services outlined in Exhibit A 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 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 an entity that is not the Provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF PII

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA 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 or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

____ As soon as commercially practicable

_____By (Insert Date]

4. Signature

_____
(Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____ _____
Authorized Representative of Company Date