MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT VERSION (2018)

Cambridge Public Schools

and

Illuminate Education, Inc.

November 1, 2018

This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Cambridge Public Schools (hereinafter referred to as "LEA") and Illuminate Education, Inc. (hereinafter referred to as "Provider") on November 1, 2018. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and "Exhibit A"; and

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

WHEREAS, in order to provide the Services described in Article 1 and Appendix 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 Federal 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. 6501-6502; 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.; and

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

WHEREAS, the Parties wish to enter into 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 state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. 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 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. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described in "Exhibit A", which are subject to change based on LEA's subsequent order(s) of Provider's products and/or services.

3. **Student Data to Be Provided**. In order to perform the Services described in this Article, LEA shall provide the categories of data described in the Schedule of Data, attached hereto as "Exhibit B", which LEA shall be solely responsible for adhering thereto.

4. **DPA Definitions**. The definition of terms used in this DPA is 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, a 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 this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). 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 Agreement 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 notwithstanding the above. The LEA will have access and be able to download its Student data at all times during the term of the contract for Services. 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 personally identifiable information on 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 will have access and be able to download its Student data at all times during the term of the contract for Services. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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.

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 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 or the Provider is reasonably unable to give advance notice under the given circumstances. 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 Nonetheless, The Provider may assign to any successor through merger, sale or other disposal method its obligations and rights under this Agreement. The Provider must require the successor to assume all obligations of this

Agreement. In the event that the Provider anticipates selling, merging or otherwise disposing of its business to a successor during the term of the Agreement, the Provider shall provide written notice of the sale, merger or disposal to the LEA no later than sixty (60) days after the sale, merger or disposal is publicly announced. Such notice shall include a written, signed assurance that the successor will assume the obligations of the Agreement. The LEA has the authority to terminate the Agreement if it disapproves of the successor to whom the Provider is selling, merging or otherwise disposing of its business, which shall only be reasonably exercised.

Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous and/or de-identified usage of data.

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 this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with 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 DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA. LEA shall ensure 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 Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.

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 student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified and/or aggregate information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all of Provider's internal security procedures to remain compliant with all applicable state and federal laws. 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 and/or aggregate 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 and/or aggregate 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 (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. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

5. **Disposition of Data**. Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA in no event longer than thirty days. 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.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising 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; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service.

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 are not limited to:

a. **Passwords and Employee Access**. Provider shall secure Provider-issued usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by 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.

b. **Destruction of Data.** Provider shall destroy Student Data, upon the written request of the LEA. 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 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 DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA. 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 security training to those of its employees who operate or have access to the system, as required under the law. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions, which shall be LEA's assigned account manager or the legal department (contracts@illuminateed.net).

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 data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.

f. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data.

g. **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.

h. **Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit non-confidential documentation pertaining to security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof to the extent available to Provider. The Provider will cooperate fully with the LEA and any state, or federal agency with oversight authority/jurisdiction in connection with any state or Federal audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to records in the Provider's possession pertaining to the Provider, LEA and delivery of Services to the Provider.

i. **Data Breach**. In the event that Student Data is accessed, Provider shall provide prompt notification to LEA within ten (10) days of confirmation of a data breach. Provider shall provide the following at the time of notification:

a. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA 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. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

v. Provider agrees to adhere to all requirements in the Massachusetts Data Breach law 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.

b. 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 employees, upon request at reasonable times to answer questions on non-confidential information in the written incident response plan.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for 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 and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

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

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, 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 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:

Name	Jeffrey Dress
Title	Vice President of Legal
Address	6531 Irvine Center Drive, Suite 100 Irvine, CA 92618
Telephone Number	949-656-3133
Email	contracts@illuminateed.net

The designated representative for the LEA for this Agreement is:

Steve Smith
Chief Information Officer
Information, Communications, and Technology Services
Cambridge Public Schools
459 Broadway, Cambridge, MA 02138
617.349.3055 | ssmith@cpsd.us

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to handling Student Data. 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**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN

ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, 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 MIDDLESEX 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, 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.

10. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

    Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

    If either party would like a paper copy of this Agreement, they may request a copy from the other party.

11. **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. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

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 any other school district who signs the acceptance in said Exhibit.

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

CAMBRIDGE PUBLIC SCHOOLS

_____ Date: 5-28-19

Printed Name: Kenneth N. Salim, Ed.D. Title: Superintendent of Schools

ILLUMINATE EDUCATION, INC.

_____ Date: May 24, 2019

Printed Name: Jeffrey Dress Title: Vice President of Legal

EXHIBIT A

DESCRIPTION OF SERVICES

An online student achievement platform. Student assessment and data management software.

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.	X
	Other application technology meta data-Please specify:	Browser Version
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	X
	Other assessment data-Please specify:	Local Test Scores
Attendance	Student school (daily) attendance data	X
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	Per district request
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	X
	Other enrollment information-Please specify:	Entry/Exit Dates
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
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	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify:	Per district request
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	
	Phone	
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
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)	X
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	
Student work	Student generated content; writing, pictures etc.	X
	Other student work data - Please specify:	Notes entered during assessment
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

	Other transportation data - Please specify:	

Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT C DEFINITIONS

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. 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, include but are not limited to blurring, masking, and perturbation. Aggregate information is student data that has obscured any PII by combining the data in some form and/or subset of the data. De-identification and aggregate information should ensure that any information when put together cannot indirectly identify the student.

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" is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. It also includes all information, including recordings and computer tapes, microfilm, microfiche, or any other materials regardless of physical form or characteristics concerning a student that is organized on the basis of the student's name or in a way that such student may be individually identified, and that is kept by the public schools of the Commonwealth. It includes standardized test results, class rank (when applicable), extracurricular activities, and evaluations by teachers, counselors, and other school staff.

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 includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is a student's personally identifiable information.Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts 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: 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: (1) uses for data collection, analytics, storage, or other service to operate and/or improve its software; and (2) who has access to PII.

Third Party: The term "Third Party" means an entity that is not the Provider or LEA.