NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT
VERSION (2019)

Concord School District

and

EDpuzzle, Inc.

September 9, 2019

This New Hampshire Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Concord School District (hereinafter referred to as "LEA") and EDpuzzle, Inc. (hereinafter referred to as "Provider") on September 9, 2019. 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 New Hampshire 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 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 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 state privacy statutes, including the 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 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".

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

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 Provider will cooperate and provide Student Data within ten (10) days at 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 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. Provider shall cooperate and respond within ten (10) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. 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.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account. Except as otherwise provided in the laws, the aforementioned shall not apply if proven to be incompatible with the Service, technically impossible or to involve a disproportionate effort for Provider.

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 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 this DPA, whereby the Subprocessors commit to secure and protect Student Data in manner consistent with the terms of this DPA. Without prejudice to the aforementioned, contracting Subprocessors for supporting Provider's business shall not be subject to the District's consent or authorization.

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, 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. 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 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 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 (a) it fits into the de-identified information exception in Article IV, Section 4; (b) re-disclosure is made to Subprocessors contracted by Provider for supporting Provider's business in accordance with Article II, Section 6; 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 applicable provisions of this DPA with respect to the 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 pursuant to the DPA.

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). 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. Transfer of de-identified Student Data shall not be subject to the aforementioned restrictions when transfer is made to Subprocessors contracted by Provider to support Provider's business and only to that extent. Provider shall not copy, reproduce or transmit any 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 or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. The LEA will have the ability to download names, responses, results and grades obtained by students in their assignments (*i.e.*, student gradebooks) at any point prior to deletion. Return or transfer of data, other than the names, responses, results and grades obtained by students in their assignments, to LEA shall not apply if proven to be incompatible with the Service, technically impossible or to involve a disproportionate effort for Provider. In such events, and upon written request by LEA, Provider shall proceed to deletion of personally identifiable information in a manner consistent with the terms of this DPA, unless prohibited from deletion or required to be retained under state or federal law. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Nevertheless, Provider may keep copies and/or backups of personally identifiable

information as part of its disaster recovery storage system, provided personally identifiable data is (a) inaccessible to the public; (b) unable to be used in the normal course of business by Provider; and (c) deleted after a maximum term of thirteen (13) months since the creation of said copies and/or backups. In case such copies and/or backups are used by Provider to repopulate accessible data following a disaster recovery, the Provider will provide fifteen (15) days' notice to the LEA and the LEA shall be entitled to demand from Provider the immediate deletion of said copies and/or backups, by sending a written request by either regular or electronic mail at privacy@edpuzzle.com. 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. Provider agrees, upon written request by LEA, to provide written notification of data destruction to LEA. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D"). Where applicable, upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said 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, 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 Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by 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 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 or, where possible, transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable 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 that meet industry best 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 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, except as necessary to fulfill the purpose of data requests by LEA. 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 system. 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, Provider shall provide LEA, upon written request by LEA, with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, 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. **Security Coordinator**. Provider shall, upon written request by LEA, 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 commit to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

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.** At least once a year, except in the case of a verified breach, 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. 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 and LEA's Student Data and all records pertaining 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 Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and no later than within ten (10) days of the incident. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "When it Occurred," "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 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. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

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

c. At LEA's discretion, the security breach notification may also include any of the following:

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

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in the New Hampshire 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.

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 and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for one (1) year.

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.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy, upon written request by LEA, all of LEA's data pursuant to Article V, section 1(b). In the absence of written request, student data shall be automatically deleted after user accounts have been inactive por a period of eighteen (18) months.

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, 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 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:

   Jordi Gonzalez
   Product Manager | EDpuzzle, Inc.
   Av. Pau Casals 16, Ppal. 2-B, 08021 Barcelona, Spain
   (0034) 936 749 140
   privacy@edpuzzle.com

   The designated representative for the LEA for this Agreement is:

   Pam McLeod, CETL
   Director of Technology | Concord School District
   38 Liberty Street, Concord, NH 03301
   (603) 225.0811 | pmcleod@sau8.org

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 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 MERRIMACK 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. **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. **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 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 the 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.

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

[*Signature Page Follows*]

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

CONCORD SCHOOL DISTRICT

By: Pamela McLeod (Sep 30, 2019) Date: 9/30/2019

Printed Name: Pamela R McLeod Title/Position: Director of Technology

EDPUZZLE, INC.

By: Jordi Gonzalez Date: 09/12/2019

Printed Name: Jordi Gonzalez Title/Position: Product Manager

EXHIBIT "A"

DESCRIPTION OF SERVICES

Edpuzzle is a simple, easy-to-use video platform that helps teachers engage their students. In the classroom, teachers use Edpuzzle to impart video-lessons their students watch through the Edpuzzle Apps (iOS and Android), the Edpuzzle website (www.edpuzzle.com) or the Learning Management System with which Edpuzzle has been integrated (Canvas, Moodle, Schoology, etc.). Beyond the classroom, teachers use Edpuzzle to engage students at home and complete the video-learning experience anywhere. Teachers can instantly collect students' viewing history and responses to embedded questions.

Edpuzzle teachers can either upload their own videos, use the ones posted on YouTube or re-use an already existing video-lesson created by another teacher. Then, teachers may edit the video to create their lessons. They may record their voice to personalize it and hold their students accountable by embedding questions in the video. Finally, teachers will assign the video to their students and follow their progress in real time while they all learn at their own pace.

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:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	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	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	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)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	X (ONLY TO TEACHER GENERATED SURVEYS)

Category of Data	Elements	Check if used by your system
Student work	Student generated content; writing, pictures etc.	X (DEPENDANT ON TEACHER ASSIGNMENTS)
	Other student work data - Please specify:	
Transcript	Student course grades	X
	Student course data	
	Student course grades/performance scores	X
	Other transcript data - Please specify:	
Transportation	Student bus assignment	

Category of Data	Elements	Check if used by your system
	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 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" shall include, but are not limited to, student data, metadata, and user or pupil-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, without limitation, at least 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-generated content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

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 descriptive 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 Agreement, 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: 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 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 DATA

[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

OPTIONAL: EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? **x Yes** □ No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

____ CIS Critical Security Controls

____ NIST Framework for Improving Critical Infrastructure Security

X Other: OWASP Open Web Application Security Project

Online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the fields of web application security. It was started in 2001 as a non-profit organization and since its foundation it has contributed with a wide range of publications. Edpuzzle has embraced most of the OWASP recommendations, in regard to authentication and related topics. In order to comply with OWASP practices, the security engineering team has instituted a task force to conduct a detailed review of the current status of the company's solutions and to determine features that can be improved or added. At the moment, Edpuzzle's practices align with the following OWASP recommendations:

- Authentication
- Access Control
- Code Injection
- Security Misconfiguration

3. Does your organization store any customer data outside the United States? **x Yes** □ No

4. Does your organization encrypt customer data both in transit and at rest? **x Yes** □ No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Chief Security Officer

Contact information: privacy@edpuzzle.com

6. Please provide any additional information that you desire.

Edpuzzle Security Policy

EDpuzzle, Inc.

Address (for notification purposes):
Av. Pau Casals 16, Ppal. 2-B,
08021 Barcelona, Spain
privacy@edpuzzle.com

Personnel Security

Edpuzzle's personnel practices apply to all members of the Edpuzzle workforce ("Edpuzzle") – regular employees, independent contractors and interns ("employees") – who have direct access to Edpuzzle's internal information systems ("systems") and/or unescorted access to Edpuzzle's office space. All employees are required to understand and follow internal policies and standards.

Onboarding and Offboarding Practices

Before gaining initial access to systems, all employees must:

(1) Agree to confidentiality terms and equipment policies.
(2) Pass a criminal background check.
(3) Undergo a security training. This training covers privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management and incident reporting.

Upon termination of employment at Edpuzzle, all access to Edpuzzle is removed immediately and all devices provided by Edpuzzle are returned to the Company.

Security and Privacy Training

During their tenure, all employees are required to complete a refresh of privacy and security training at least annually. They are also required to acknowledge that they have read and will follow Edpuzzle's information security policies at least annually. Some employees, such as engineers, operators and support personnel who may have elevated access to systems or data, will receive additional job-specific training on privacy and security. Edpuzzle may also test employees to ensure they have fully understood security policies.

Employees are required to report security and privacy issues to appropriate internal teams in accordance with Edpuzzle's Incident Response Plan ("IRP"). Employees are informed that failure to comply with acknowledged policies may result in consequences, up to and including termination of the employment agreement.

Authorizing Access

To minimize the risk of data exposure, Edpuzzle adheres to the principle of least privilege – employees are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. To ensure that users are so restricted, Edpuzzle employs the following measures:

(1) All systems used at Edpuzzle require users to authenticate, and users are granted unique identifiers for that purpose.
(2) Each user's access is reviewed at least quarterly to ensure the access granted is still appropriate for the user's current job responsibilities.

Workers may be granted to access to a small number of internal systems by default upon hire. Request for additional access follow a documented process and must be approved by the responsible owner or manager.

Authentication

Edpuzzle requires personnel to use the provided password manager. Password managers generate, store and enter unique and complex passwords. Use of the password manager helps avoid password reuse, phishing, and other security threats. Any password stored or shared through any other means will be considered a data breach and affected accounts might be suspended at any time.

Third-Party Services Review

Any tools, projects, or vendor agreements that involve sharing sensitive data (intellectual property, proprietary source code, or subscriber data) must go through a security review before being implemented. When employees and/or contractors of the Company need to use external solutions, they must fill out a form that thoroughly specifies all the details of the solution. For example, they must input:

(1) Why this solution and this vendor is needed.
(2) The members of Edpuzzle's workforce who will use the solution.
(3) The list of Edpuzzle's data and/or access that will be shared.

With this information, the Security Team reviews the objectives, the members involved in the solution's usage, and what data will be exchanged with the vendor before deciding on whether to proceed with its implementation.

Organizational Security

Dedicated Security Professionals

Edpuzzle has defined roles and responsibilities to delineate which roles in the organization are responsible for operating the various aspects of security.

Audits, Compliance and Third-Party Assessments

Edpuzzle operates a comprehensive security program designed to address the vast majority of the requirements of common security standards in the field of education including, but not limited to, FERPA, COPPA and the EU-US Privacy Shield.

Protecting User Data

The focus of Edpuzzle's security program is to prevent unauthorized access to user data. To this end, our team of dedicated security practitioners, working in partnership with peers across all our teams, take exhaustive steps to identify and mitigate risks, implement best practices and constantly evaluate ways to improve.

Privacy Policies

Edpuzzle limits the private data we collect and what we do collect is detailed in our Privacy Policy. Personal information is requested only when it is required to deliver expected services and to ensure that the Company site and solutions run properly. When we analyze our users' data we use aggregated data pools to protect the privacy of individual subscribers.

As stated in the Privacy Policy, Edpuzzle is also certified and follows the rules laid out in the FERPA, COPPA and European GDPR. Among others, Edpuzzle must:

- Make clear to individuals what type of data is collected, and for what purposes.
- Inform individuals of any third parties to whom their data will be transferred, their right to access their data, and the means for limiting the use and disclosure of their personal data.
- Enable individuals to opt out of any disclosure of personal data to a third party or the use of data for a purpose other than the one for which it was initially collected.
- Specify, in third party contracts, that transferred personal data may only be processed for limited and specified purposes consistent with the data subject's consent.
- Take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- Do not collect personal data for students under thirteen (13) unless we have parental or school consent.
- Delete account and personal identifiable information after eighteen (18) months of inactivity.

Prior to making material changes in the Privacy Policy, Edpuzzle commits to:

(1) Notify schools about new or additional data collection or practices in a "click wrap agreement".
(2) Ensure that third-party services are capable of complying with new practices and guidelines.

Third-Party Services Compliance

Edpuzzle assesses the privacy and security policies and practices of third-party service providers. To that effect, we have agreements in place with them to ensure that they are capable of complying with Edpuzzle's practices and policies. Such procedures must be repeated at least on an annual basis.

Edpuzzle only sends personal identifiable information to third-party services that are required to fully attend our users' needs, which are the following:

- Amazon Web Services
- Marketo
- Mixpanel
- MongoDB Atlas
- Quickbooks
- Salesforce

- Stripe
- Zendesk

Controlling change

To minimize the risk of data exposure, Edpuzzle controls changes, especially changes to production systems, very carefully. These change-control-requirements are designed to ensure that changes potentially impacting user data are documented, tested, code reviewed and approved before deployment:

- Documented: any employee aiming to insert changes to our production systems should create a task, subtask or project in our approved task manager indicating the purpose of the changes, for both technical and non-technical audiences, and any other relevant information that may help co-workers to better understand the scope and impact of the task. It should be clear who will take part in these changes by properly setting the task, subtask or project assignee and followers. More documentation may be required upon deep changes.

- Tested: all code that may fetch, modify or remove data from our systems should be fully tested, paying special attention to authentication and authorization restrictions to ensure that there's no unauthorized release, disclosure or acquisition of personal information.

- Code reviewed: human errors are a well-known source of security issues. For this reason, all components developed by Edpuzzle are reviewed at least by another engineer – with a reasonable level of seniority – to ensure security, performance, and adherence to the company principles and commitments.

- Approved: prior to release, security teams and managers must be notified about the changes that are intended to be shipped so that they can effectively carry out their duties including, but not limited to, monitoring. Should this release be believed to compromise the security of the users, the security teams and the managers reserve the option to cancel or delay the changes.

Data Protection Impact Assessments

With the entry into force of the European General Data Protection Regulation (GDPR), Edpuzzle has also introduced the drafting of Data Protection Impact Assessments (DPIAs) as an indispensable and mandatory step before making any changes to the Service effective (art. 35 GDPR).

DPIAs are drafted by Edpuzzle's Data Protection Officer (DPO) and they analyze the impact of eventual changes or new projects on user privacy. In case any risks to that privacy are detected during the assessment, measures to minimize or eliminate the risks are proposed by the DPO. Proposed measures are then discussed with Product Management and, depending on the urgency and dimension of the risks, other departments may be asked to intervene.

Finally, measures to either reduce or eliminate detected risks are implemented prior to making the eventual changes effective.

OWASP Compliance

The Open Web Application Security Project (OWASP) is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the fields of web application security. It was started in 2001 as a non-profit organization and since its foundation it has contributed

with a wide range of publications. Edpuzzle has embraced most of the OWASP recommendations in regards to authentication and related topics. In order to comply with OWASP practices, the security engineering team has instituted a task force to conduct a detailed review of the current status of the company's solutions and to determine features that can be improved or added.

At the moment, Edpuzzle's practices align with the following OWASP recommendations:

- Authentication
- Access Control
- Code Injection
- Security Misconfiguration

Responding to Security Breaches

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we cannot guarantee the security of information to that extent. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time.

Initial Notice

Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of personal information, we will notify electronically, not later than 48 hours or 1 business day, such discovery to all affected users (if contact information was provided), schools and districts so that you can take appropriate protective steps. This initial notice will include, to the extent known at the time of the notification, the date and time of the breach, its nature and extent, and the Service's plan to investigate and remediate the breach. Schools and districts will also be provided with a list of students and employees whose data was released, disclosed or acquired.

Detailed Notification

Upon discovery of a breach, we will conduct a deep investigation in order to electronically provide, not later than 5 calendar days, all affected users (if contact information was provided), schools and districts with a more detailed notice of the breach, including but not limited to the date and time of the breach; nature and extent of the breach; and measures taken to ensure that such breach does not occur in the future. Schools and districts will also be provided with the name(s) of student(s) and employee(s) whose data was released, disclosed or acquired. We may also post a notice on our homepage (www.edpuzzle.com) and, depending on where you live, you may have a legal right to receive notice of a security breach in writing.

Data Removal

Period of Inactivity

Any account that has been inactive for more than 18 months will be de-identified (from now on "removed") through a daily automated script, from our systems and any other third-party services. The devops team is in charge of monitoring the proper performance of the script and is committed to notify the Data Protection Officer immediately if any data is not removed as expected.

Explicit Requests

Upon data removal request via any available channel (twitter, employee email, support email, phone, video call or in person) employees must make sure this request is properly received by the Data Protection Officer (DPO) immediately. To this end, employees will create a ticket in our approved CRM and assign it to the DPO, who will be checking any new petitions on a daily basis.

By reasonable means, the DPO will determine if the requester has proper authorization for these actions, depending on the requester role:

- Teachers: assuming that the Principal, Superintendent or IT Admin have approved such intentions, this personnel will have the right to delete any data from students in their classrooms. Please note that a student can be linked to various classrooms from different teachers.

  To delete their own account or any other data, they should proceed from the EDpuzzle Web interface.

- Principals, Superintendents or IT Admins: this personnel is considered to have the highest authorization in a school/district and will have the right to delete any employees or students data they ask for.

- Students: DPO will not directly attend to any students request and will redirect them to their teacher or school/district instead to avoid data removal for cheating purposes and to ensure the school/district has been properly notified about this request.

- Parents: DPO will not directly attend to any parents request and will redirect them to their teacher or school/district instead to ensure the school/district has been properly notified about this request.

Once the authorization is granted, Edpuzzle will proceed to permanently remove the requested data from its systems, including but not limited to servers, workstations and storage media. Edpuzzle will also make sure this data is permanently removed from any third-party system it may have been shared with.

Edpuzzle will complete the request not later than 48 hours since the authorization was granted.

Security backups

Edpuzzle regularly makes and keeps copies/backups of data as part of its disaster recovery storage system. The information contained in said copies/backups is inaccessible to the public and unable to be used in the normal course of business by Edpuzzle. Further to that, all copies/backups are automatically deleted after a maximum term of thirteen (13) months.

HELLOSIGN

Audit Trail

TITLE	Concord Public Schools - NH_NHSDPA
FILE NAME	EDPuzzle_ConcordNH.pdf
DOCUMENT ID	8b2674d740ecefee0b25bc312250e25a2387bc3d
STATUS	Completed

Document History

SENT	**09/09/2019** 12:50:25 UTC	Sent for signature to Jordi González (jordi@edpuzzle.com) from julia@edpuzzle.com IP: 88.12.43.131
VIEWED	**09/12/2019** 14:56:14 UTC	Viewed by Jordi González (jordi@edpuzzle.com) IP: 88.12.43.131
SIGNED	**09/12/2019** 15:05:07 UTC	Signed by Jordi González (jordi@edpuzzle.com) IP: 88.12.43.131
COMPLETED	**09/12/2019** 15:05:07 UTC	The document has been completed.