DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the "Agreement") is made and entered into by and between EDpuzzle, Inc. (the "Vendor") and **Cuba-Rushford Central School** ("CRCS").

WHEREAS, CRCS and Vendor are parties to an underlying agreement composed of the Vendor's Terms of Service and Privacy Policy, both accessible at https://edpuzzle.com/terms and https://edpuzzle.com/privacy, respectively (hereinafter jointly referred to as the "Contract") pursuant to which the Vendor will receive student data and/or teacher or principal data ("Protected Data") that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from CRCS for purposes of providing certain products or services to CRCS. To the extent that any terms contained in the Contract, or any terms contained in any other document(s) attached to and made part of it, conflict with the other terms of this Agreement, the terms of this Agreement shall apply and be given effect; and

WHEREAS, both CRCS and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

NOW THEREFORE, in consideration of the mutual promises and covenants contained in the Contract, as well as, this Agreement the parties hereto mutually agree as follows:

1. **Confidentiality**

    a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided for in the Contract is deemed confidential information.

    b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with federal and state law and that any information obtained will not be revealed to any persons, firms or organizations not authorized pursuant to the Contract or this Agreement.

2. **Data Protections and Internal Controls**

    a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by CRCS that directly relate to a student(s) (hereinafter referred to as "education record").

    b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:

1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and

2. Not use the education records for any other purpose than those explicitly authorized in the Contract and/or this Agreement; and

3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

4. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

3. Data Security and Privacy Plan

a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from CRCS.

b. Vendor submits a Data Security and Privacy Plan to CRCS, attached hereto , which shall:

1. Outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with CRCS's policy on data security and privacy accessible at: 2020-2021 Data Security (sharepoint.com).

2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from CRCS under the Contract.

3. Outline the training requirement established by the Vendor for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

4. Notice of Breach and Unauthorized Release

a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:

1. Immediately notify CRCS in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or authorized release.

2. Advise CRCS as to the nature of the breach and steps Vendor has taken to minimize said breach.

b. In the case of required notification to a parent or eligible student, the Vendor shall:

1. Promptly reimburse CRCS for the full costs of such notification.

c. Vendor will cooperate with CRCS and provide as much information as possible directly to CRCS about the incident, including but not limited to:

    1. The description of the incident;

    2. The date of the incident;

    3. The date Vendor discovered or was informed of the incident;

    4. A description of the types of Protected Data involved;

    5. An estimate of the number of records affected;

    6. The schools within CRCS affected;

    7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data; and

    8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

d. The Vendor shall indemnify and hold CRCS harmless from any claims arising from its breach within the Data Sharing and Confidentiality Agreement confidentiality and data security and privacy standards provision.

e. Vendor acknowledges that upon initial notification from Vendor, CRCS, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by CRCS or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by CRCS, Vendor will promptly inform CRCS of the same.

5. Vendor Information

Vendor understands that as part of CRCS's obligations under New York Education Law Section 2-d, Vendor is responsible for providing CRCS with Vendor information (see Vendor Information for Data Privacy and Security) to include:

a. Exclusive purposes for which the student data will be used;

b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;

c. Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student;

d. Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so. Notwithstanding any of the foregoing, teachers using the service may provide express consent to receive commercial communications

e. Vendor will provide a description of what will happen to the personally identifiable information upon expiration of the written agreement (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will be destroyed).

f. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and

g. Where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

6. <u>Termination or Expiration of Contract and/or Agreement</u>

a. Upon termination of this Agreement, and written request by CRCS, Vendor shall destroy all confidential information obtained in connection with the services provided therein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. In the absence of a written request, Vendor shall destroy all confidential information upon eighteen (18) months of end-user account inactivity. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement for as long as Vendor retains possession of confidential information.

b. If requested by CRCS in writing at any point prior to data deletion, Vendor will assist CRCS in downloading names, responses, results and grades obtained by students in their assignments ("Student Gradebooks") in a standard electronic legible format (such as .csv or .json).

c. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, on any storage medium whatsoever.

d. Vendor may use de-identified Protected Data for purposes of research, the improvement of Vendor's products and services, and/or the development of new products and services. In no event shall Vendor or its Subcontractors re-identify or attempt to re-identify any de-identified Protected Data or use de-identified Protected Data in combination with other data elements or de-identified Protected

Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

e. Without prejudice to the foregoing, Vendor may retain data backups that are part of Vendor's disaster recovery storage system, for an additional term of thirteen (13) months after termination of the Contract, provided such backups remain inaccessible to the public and are unable to be used by the Vendor in the normal course of its business. Upon written request by the CRCS, Vendor will provide CRCS with a certification from an appropriate officer that these requirements have been satisfied in full.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

CRCS is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, CRCS informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to CRCS Data Privacy Officer, 5476 Route 305, Cuba, New York 14727. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

IN WITNESS WHEREOF, the parties hereto have executed this agreement on the date of the last signature affixed hereto.

Julia Trius

Authorized Vendor Signature
Julia Trius, Head of Legal

05 / 11 / 2021

Date

Noah Pfeiffer

Authorized CRCS Signature
Noah Pfeiffer, Data Protection Officer

05 / 11 / 2021

Date

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: EDpuzzle, Inc. Product: Edpuzzle instructional software

Collects: ☒ Student Data ☒ Teacher or Principal Data ☐ Does not collect either

Educational agencies including Cuba Rushford Central School are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

Part 1: Exclusive Purposes for Data Use	**RESPONSE REQUIRED**
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor. Student and Teacher Data will be used by Edpuzzle for providing and improving the service and for the following limited purposes: a. to create the necessary accounts to use the service (student accounts); b. to provide teachers with analytics on student progress; c. to send teachers email updates, if applicable; d. to help teachers connect with other teachers from the same school or district; e. to assess the quality of the service; f. to secure and safeguard personal information of other data subjects; g. to comply with all applicable laws on the protection of personal information. Edpuzzle shall not use PII for any purposes other than those authorized pursuant to the Agreement and may not use PII for any targeted advertising or other commercial uses. Nevertheless, teachers using Edpuzzle's Service may provide express consent to receive Commercial or Marketing communications.	

Part 2: Subcontractor Oversight Details	**RESPONSE REQUIRED**
☐ This contract has no subcontractors. ☒ This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law: Having agreements in place with subcontractors to ensure they abide by data protection obligations consistent with those applicable to Edpuzzle under applicable laws and regulations.	

Part 3: Contract Lifecycle Practices	**RESPONSE REQUIRED**
The contract expires as set forth in the Edupzzle's Data Security and Privacy Plan attached below: either (a) at District's request upon proactive deletion of user accounts; or (b) in the absence of any specific request or action, after eighteen (18) months of account inactivity. Deletion of student accounts must be requested by the District's authorized representative by sending a written request at support@edpuzzle.com or privacy@edpuzzle.com. When the contract expires, the following will happen to the personally identifiable information (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will	

be destroyed): personally identifiable information will be destroyed or returned as set forth in the Data Sharing and Confidentiality Agreement to which this Vendor Information is attached, and the Edpuzzle's Data Security and Privacy Plan below.

Part 4: Student Educational Records / Improper Disclosure

A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website.

B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.

Part 5: Security Practices **RESPONSE REQUIRED**

A. Protected data provided to the contractor will be stored: (include *where* and *how*)

The data is stored in externalized databases that are currently being provided by MongoDB Atlas, and simultaneously hosted on Amazon Web Services in North Virginia (United States). User-generated content (which may or not contain personal information) may be temporarily stored in other countries in order for Edpuzzle to provide a better service. Concretely, uploaded videos, audios or images may have a copy temporarily stored in other regions to reduce the time of load.

B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include: (a) pseudonymisation and encryption of data; (b) password protection; (c) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (d) restore the availability and access to personal data in a timely manner in the event of a technical incident; and (e) regularly test, assess and evaluate the effectiveness of technical and organizational measures ensuring the security of the processing.

Part 6: Encryption Practices **RESPONSE REQUIRED**

☒ By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).

DATA SECURITY AND PRIVACY PLAN FOR EDPUZZLE

1. Exclusive Purposes for Data Use
   a. Please list the exclusive purposes for which the student data [or teacher or principal data] will be used by the service provider.

   Student and Teacher Data will be used by the Service Provider for improving the Services and for the following limited purposes:

   a. to create the necessary accounts to use the Service;
   b. to provide teachers with analytics on student progress;
   c. to send teachers email updates, if applicable;
   d. to help teachers connect with other teachers from the same school or district;
   e. to assess the quality of the Service;
   f. to secure and safeguard personal information of other data subjects;
   g. to comply with all applicable laws on the protection of personal information.

   Initial: J.T.

2. Data Accuracy/Correction Practices
   a. Parents [student, eligible student, teacher or principal] may challenge the accuracy of the data by directly contacting their educational institution.

   Initial: J.T.

   Subcontractor Oversight Details

   This contract has subcontractors: Yes ☒ No ☐

   Initial: J.T.

   Describe how the contractor will ensure subcontractors abide by data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations:

   To the extent permitted by law, and as reasonably necessary to provide the Edpuzzle Service to the District, the Service Provider may provide access to, export, transfer, or otherwise disclose student and/or teacher data to the Service Provider's assignees, agents and subcontractors; provided that prior to any such disclosure, the assignee, agent or subcontractor receiving data has agreed in writing to comply with data protection obligations consistent with those applicable to the Service Provider under applicable laws and regulations.

   Initial: J.T.

3. Security Practices

   a. Where is the data stored? (described in such a manner as to protect data security)

      Data is stored in externalized databases that are currently being provided by MongoDB Atlas (security compliance information), and simultaneously hosted on Amazon Web Services (security and compliance information) in North Virginia (United States).

   b. The security protection practices taken to ensure data will be protected include:

- Pseudonymisation and encryption of PII (TLS v1.2 for all data in transit between clients and server and AES256-CBC (256-bit Advanced Encryption Standard in Cipher Block Chaining mode) for encrypting data at rest).
- Password protection.
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Restore the availability and access to personal data in a timely manner in the event of a technical incident.
- Regularly test, assess and evaluate the effectiveness of technical and organizational measures ensuring the security of the processing.

Initial: J.T.

4. Contract Lifecycle Practices
    a. The agreement expires either (a) at District's request upon proactive deletion of user accounts; or (b) in the absence of any specific request or action, after eighteen (18) months of account inactivity. Deletion of student accounts must be requested by the District's authorized representative by sending a written request at support@edpuzzle.com or privacy@edpuzzle.com.

    b. When the agreement expires,
        i. How long will the student [or teacher or principal] data be retained?

        Contractor may keep copies and/or backups of data for an additional term of thirteen (13) months after termination of the agreement as part of its disaster recovery storage system, provided such data is (a) inaccessible to the public; and (b) unable to be used in the normal course of business by the Service Provider.

        ii. How will the student data be disposed of?

        Data shall be destroyed as per best practices for data destruction using commercially reasonable care, security procedures and practices.

Initial: J.T.

5. Encryption Practices
   Data encryption is applied in accordance with Education Law 2-d 5(f)(5)

   Yes ☒ No ☐

Initial: J.T.

6. Training Practices
    a. Annual training on federal and state law governing confidentiality is required for any officers, employees, or assignees who have access to student [or teacher or principal] data

    Yes ☒ No ☐

Initial: J.T.

EDpuzzle, Inc.
Company Name

Julia Trius, Head of Legal
Print Name and Title

Julia Trius
Signature of Provider

05 / 11 / 2021
Date

HELLOSIGN

Audit trail

TITLE	Cuba Rushford_CS-NY-DPA
FILE NAME	Cuba Rushford_CS-NY-DPA.pdf
DOCUMENT ID	a1e7761cb55ce7c2622bc2364f40852badf64f39
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document history

SENT	**05 / 11 / 2021** 06:31:43 UTC	Sent for signature to Julia Trius (julia@edpuzzle.com) and Noah Pfeiffer (npfeiffer@mycrcs.org) from marta@edpuzzle.com IP: 85.57.198.130
VIEWED	**05 / 11 / 2021** 09:09:39 UTC	Viewed by Julia Trius (julia@edpuzzle.com) IP: 83.57.50.113
SIGNED	**05 / 11 / 2021** 09:11:24 UTC	Signed by Julia Trius (julia@edpuzzle.com) IP: 83.57.50.113
VIEWED	**05 / 11 / 2021** 12:21:46 UTC	Viewed by Noah Pfeiffer (npfeiffer@mycrcs.org) IP: 168.169.221.38
SIGNED	**05 / 11 / 2021** 12:50:41 UTC	Signed by Noah Pfeiffer (npfeiffer@mycrcs.org) IP: 168.169.221.38
COMPLETED	**05 / 11 / 2021** 12:50:41 UTC	The document has been completed.