

THE EAST RAMAPO CENTRAL SCHOOL DISTRICT DATA PRIVACY AGREEMENT ANNUAL NOTICE

The East Ramapo Central School District (the “District”) and you, a third-party contractor (the “Contractor”), entered into an agreement to provide services to the District. In rendering those services, the Contractor required either student personally identifiable information and/or teacher APPR data. As such, the District required the Contractor to execute a Data Privacy Agreement.

This Notice shall serve to remind the Contractor of its obligations and responsibilities set forth in the Data Privacy Agreement to act in accordance with Education Law § 2-d, and its implementing regulations under 8 NYCRR Part 121. If anything has changed since the date of execution of the Data Privacy Agreement, it is incumbent upon the Contractor to contact the District immediately to update it.

If your original Data Privacy Agreement had an end date for service, and the Parties have entered into a new Service Agreement or renewed their Service Agreement or continued with a free service under the Contractor’s Terms and Conditions, **this Notice shall serve to notify the Contractor that all obligations set forth in 8 NYCRR Part 121 still apply until the student personally identifiable information and/or teacher APPR data is returned and/or destroyed.**

As a convenience, a copy of your original executed Data Privacy Agreement has been attached to this Notice.

<u>EAST RAMAPO CENTRAL SCHOOL DISTRICT</u>	<u>CONTRACTOR</u> – EDpuzzle Inc. 2023-2024
Signature: <u><i>Bhavin gandhi</i></u> <small>Bhavin gandhi (Sep 15, 2023 09:21 EDT)</small>	Signature: <i>Jaume Bohigas</i>
Print Name: Bhavin gandhi	Print Name: Jaume Bohigas
Title: Director of Information Technology	Title: Director of Security & Infrastructure
Date: Sep 15, 2023	Date: Sep 15, 2023

EAST RAMAPO CENTRAL SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

**EAST RAMAPO CENTRAL SCHOOL
DISTRICT
and
EDpuzzle, Inc.**

This Data Privacy Agreement ("DPA") is by and between the East Ramapo Central School District, ("EA"), an Educational Agency, and EDpuzzle, Inc., a Delaware corporation ("Contractor"), collectively, the "Parties".

This DPA is a rider to the Contractor'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 "Service Agreement"), and made as of the date of the last signature affixed hereto, that governs the provision of the Edpuzzle service, a web based-instructional software providing video-editing tools and student progress analytics, accessible at <https://edpuzzle.com> (the "Services") to the EA. To the extent that any terms contained in the Service Agreement, or any terms contained in any other document(s) attached to and made part of the Service Agreement, conflict with the terms of this DPA, the terms of this DPA shall apply and be given effect.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** Means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **De-Identified Data:** Data that has had all direct and indirect identifiers removed.
4. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.

5. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
6. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
7. **Eligible Student:** A student who is eighteen years of age or older.
8. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
9. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
10. **Parent:** A parent, legal guardian or person in parental relation to the Student.
11. **Personally Identifiable Information (PII):** Means student personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
12. **Release:** Shall have the same meaning as Disclose.
13. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
14. **Student:** Any person attending or seeking to enroll in an Educational Agency.
15. **Student Data:** Personally identifiable student information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
16. **Student Gradebooks:** names, responses, results and grades obtained by Students in their assignments.
17. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.

- 18. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide the Services to the EA pursuant to the Service Agreement of even date herewith, Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices. Where such audit report is not available, Contractor will allow the EA, upon receipt of a written request and at EA's expense, to audit the security and privacy measures that are in place to ensure the protection of PII or any portion thereof. The Contractor will cooperate fully with the EA and provide access to staff, agents, reports and records as necessary for performing the audit. Audits conducted by EA under this provision shall not exceed one (1) per annum and must be: (i) conducted during Contractor's regular business hours; (ii) carried out in a manner that prevents unnecessary disruption to Contractor's operations; and (iii) subject to reasonable confidentiality procedures.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees comply with the terms of this DPA and that subcontractors abide by terms consistent with those outlined herein.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the data security and privacy requirements of this DPA, Contractor shall remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any unauthorized party not authorized pursuant to this DPA or the Service Agreement, unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA. Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA as prescribed in this DPA and the Service Agreement, unless such retention is authorized for a prescribed period of time by this DPA or the Service Agreement.
- (b) Upon expiration or termination of the Service Agreement and written request by the EA, Contractor shall assist the EA in downloading Student Gradebooks at any point prior to data deletion, in a standard exportation format such as, but not limited to, .csv or .json. Except as may be otherwise provided in applicable laws, return or transfer of data, other than Student Gradebooks, to the EA, shall not apply if proven to be incompatible with the Service, technologically impossible or to involve a disproportionate effort for the Contractor.
- (c) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, and except for backups of data that are part of Contractor's disaster recovery storage system, Contractor shall, upon written request by the EA, ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. In the absence of the abovementioned written request, Contractor shall destroy all PII upon eighteen (18) months of end-user account inactivity. Notwithstanding the foregoing, Contractor may keep backups of data as part of its disaster recovery storage system for an additional term of six (6) months after termination of services, provided such data remains inaccessible to the public and is unable to be used by the Contractor in its normal course of business. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data

destruction.

- (d) Upon written request by the EA, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor.
- (e) To the extent that Contractor and/or its subcontractors continue to be in possession of any De-Identified Data, they agree not to attempt to re-identify De-Identified Data and not to transfer De-Identified Data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose. Nevertheless, teachers using Contractor's service may provide express consent to receive Commercial or Marketing Communications by enabling (opt-in) or disabling (opt-out) them through their account's settings page.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay, and in no event no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, by e-mail transmission to the contact person provided in paragraph b) below, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's Data Protection Officer referred to in paragraph b) below. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to the EA at the following address:
 - Name: Bhavin Gandhi
 - Title: Data Protection Officer
 - Address: 105 S. Madison Avenue City, State, Zip: Spring Valley, NY 10977
 - Email: DPO@ercsd.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA. Any costs incidental to the required cooperation or participation of the Contractor or its Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive for as long as Contractor retains possession of PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS**1. Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original

signature, as if all parties had executed a single original document.

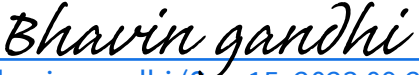

EDUCATIONAL AGENCY	CONTRACTOR
BY:  <u>Bhavin gandhi (Sep 15, 2023 09:21 EDT)</u>	BY: 
Bhavin Gandhi	Jaume Bohigas
Director of Information Technology & Cyber Security	Director of Security and Infrastructure
Date: Sep 15, 2023	Date: Sep 15, 2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

The East Ramapo Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information in educational records from unauthorized access or disclosure in accordance with Education Law§ 2-d, and all other applicable State and Federal laws.

The East Ramapo Central School District establishes the following Parents' Bill of Rights in which parents, legal guardians, persons in parental relationships, and/or Eligible Students, can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law§ 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA to: Bhavin Gandhi, Data Protection Officer at DPO@rcsd.org or 845-577-6081; (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-

[security/report-improper-disclosure](#), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	<i>Jaume Bohigas</i>
[Printed Name]	Jaume Bohigas
[Title]	Director of Security and Infrastructure
Date:	Sep 15, 2023

EXHIBIT B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY
- SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE
PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	EDpuzzle, Inc.
Description of the purpose(s) for which Contractor will receive/access PII	<p>Student and Teacher Data will be used by Edpuzzle for providing and improving the service and for the following limited purposes:</p> <ul style="list-style-type: none"> 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. <p>Edpuzzle shall not use PII for any purposes other than those authorized pursuant to the DPA and the Service Agreement and may not use PII for any targeted advertising or other commercial uses. Nevertheless, teachers utilizing the Edpuzzle service may provide express consent to receive marketing or commercial communications from Edpuzzle.</p>
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> IXI Student PII <input type="checkbox"/> APPR Data
Contract Term	<p>Contract Start Date: upon signature hereof.</p> <p>Contract End Date: upon termination of services.</p>

<p>Subcontractor Written Agreement Requirement</p>	<p>Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by state and federal laws and regulations, and the Contract. (check applicable option)</p> <p><input type="checkbox"/> Contractor will not utilize subcontractors.</p> <p>IXI Contractor will utilize subcontractors.</p>
<p>Data Transition and Secure Destruction</p>	<p>Upon expiration or termination of the Service Agreement, Contractor shall:</p> <ul style="list-style-type: none"> • To the extent compatible with the service, and as outlined in the DPA, securely assist the EA with the transfer of Student Gradebooks to EA, at the EA's option and written discretion, in a standard electronic legible format (such as, but not limited to .csv or .json). • Thereafter, securely delete and destroy data, either upon written request by the EA or upon (18) months of end-user account inactivity, except for backups of data that are part of Contractor's disaster recovery storage system which may be retained for an additional term of six (6) months after termination of services, subject to the terms set forth in the DPA.
<p>Challenges to Data Accuracy</p>	<p>Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within thirty (30) days of receiving the EA's written request.</p>

<p>Secure Storage and Data Security</p>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p>IXI Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>The data is stored in externalized databases that are currently being provided by MongoDB Atlas, and simultaneously hosted on Amazon Web Services in Northern Virginia (United States).</p> <p>User-generated content (which may or may not contain personal information) may be temporarily stored in other countries in order for Contractor 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. This would happen if, for</p>
--	--

	example, a user accessed the Services from Europe and displayed a video created by an American teacher. In such a case, a temporary copy of such media would be hosted on the European server Amazon Web Services has in that region.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	<i>Jaume Bohigas</i>
[Printed Name]	Jaume Bohigas
[Title]	Director of Security and Infrastructure
Date:	Sep 15, 2023

EXHIBIT C-CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. **For every contract, the Contractor must complete the following OR provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See attached DPSP.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See attached DPSP.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See attached DPSP.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	See attached DPSP.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See attached DPSP.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See attached DPSP.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See attached DPSP.
8	Outline how your data security and privacy program/practices <u>align</u> with the EA's applicable policies.	See attached DPSP.

g	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1. https://www.nist.gov/cyberframework/new-framework	See attached DPSP.
---	---	--------------------

Data Security and Privacy Plan

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: JB

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: JB

3. Subcontractor Oversight Details

- a. This contract has subcontractors:

Yes No

Initial: JB

- b. 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: JB

4. 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 Northern Virginia (United States).

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

- Pseudonymization and encryption of PII (TLS v1.2 and v1.3 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 JB

5. 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 six (6) 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: JB

6. Encryption Practices

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

Yes No

Initial: JB

7. 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: JB

EDpuzzle, Inc.	
[Signature]	<i>Jaume Bohigas</i>
[Printed Name]	Jaume Bohigas
[Title]	Director of Security and Infrastructure
Date:	Sep 15, 2023









ERCSD_EdpuzzleInc_Notice_DPA

Final Audit Report

2023-09-15

Created:	2023-09-12
By:	Jan Albert Sasal (jan@edpuzzle.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIpVL06dtS0RVkqfIFoEUJfmAEI7pRVal

"ERCSD_EdpuzzleInc_Notice_DPA" History

-  Document created by Jan Albert Sasal (jan@edpuzzle.com)
2023-09-12 - 1:25:06 PM GMT
-  Document emailed to Jaume Bohigas (jaume@edpuzzle.com) for signature
2023-09-12 - 1:38:15 PM GMT
-  Document e-signed by Jaume Bohigas (jaume@edpuzzle.com)
Signature Date: 2023-09-15 - 1:15:13 PM GMT - Time Source: server
-  Document emailed to bgandhi@ercsd.org for signature
2023-09-15 - 1:15:14 PM GMT
-  Email viewed by bgandhi@ercsd.org
2023-09-15 - 1:21:13 PM GMT
-  Signer bgandhi@ercsd.org entered name at signing as Bhavin gandhi
2023-09-15 - 1:21:45 PM GMT
-  Document e-signed by Bhavin gandhi (bgandhi@ercsd.org)
Signature Date: 2023-09-15 - 1:21:47 PM GMT - Time Source: server
-  Agreement completed.
2023-09-15 - 1:21:47 PM GMT