NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

St. John the Baptist Diocesan High School

and

EDpuzzle, Inc.

This Data Privacy Agreement ("DPA") is entered into as of the date of the last signature affixed hereto by and between the **St. John the Baptist Diocesan High School** ("EA"), an Educational Agency, and **EDpuzzle, Inc.**, a Delaware corporation, ("Contractor"), each a "Party" and collectively, the "Parties".

This DPA supplements the Service Agreement, as such term is defined in Article I below.

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 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. **Service Agreement:** Contractor's Terms of Service and Privacy Policy, both accessible at https://edpuzzle.com/terms and https://edpuzzle.com/privacy, respectively.
15. **Student:** Any person attending or seeking to enroll in an Educational Agency.
16. **Student Data:** 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.
17. **Student Gradebooks:** Names, responses, results and grades obtained by students in their assignments.
18. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
19. **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 certain services ("Services") to the EA pursuant to the Service Agreement of even date herewith; Contractor may receive PII regulated by several 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 written request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. These 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 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 sole expense, to audit the security and privacy measures that are in place to ensure the protection of PII or any portion thereof, provided that such audit is: (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. 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.

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 who need to know the PII comply with the terms of this DPA.

(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 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 other party not authorized pursuant to this DPA and 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 officers 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. Furthermore, Contractor shall ensure that Subcontractors abide by terms consistent with those outlined herein, including, but not limited to, the obligation to provide their officers or employees with training on the applicable laws governing confidentiality of PII.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its Subcontractors 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, and Contractor agrees that, except for backups that are part of its disaster recovery storage system, 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, unless such retention is either expressly authorized for a prescribed period by the Service Agreement, this DPA, or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. Data backups that are part of Contractor's disaster recovery storage system may be kept for an additional term of up to three (3) months after the Service Agreement's termination, provided such backups remain inaccessible to the public and are unable to be used by Contractor in the normal course of its business. As applicable, at any point prior to data deletion and upon written request by the EA, Contractor shall assist the EA with the download of Student Gradebooks in a standard exportation format such as, but not limited to, .csv or .json .

(b) If applicable, once the download of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to destroy all PII upon written request by the EA or when the purpose that necessitated its receipt by Contractor has been completed, which, in the absence of the aforementioned written request, will be deemed to occur upon eighteen (18) months of end-user account inactivity. Thereafter, 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, except for the above mentioned data backups, Contractor shall 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. 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.

(c) 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 or Subcontractors.

(d) 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. Notwithstanding any of the foregoing, teachers using the service may provide express consent to receive commercial communications by enabling (opt-in) or disabling (opt-out) them upon account creation or through their account's setting 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 no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be made by e-mail transmission 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 point of contact specified 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:

Eric Besendorfer

Director of Information Technology

1170 Montauk Hwy

West Islip, NY 11795

DataPrivacy@sjbdhs.org

13. Cooperation with Investigations.

Contractor agrees that it will use its commercially reasonable efforts to cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. 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 documented 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 any termination of this DPA and shall remain in full force and effect 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 promptly 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, as amended from time to time, 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: EDpuzzle, Inc.**
BY: ***[Signature]***	BY: ***[Signature]***
Eric Besendorfer	**Jaume Bohigas**
Director of Information Technology	**Director of Security and Infrastructure**
Date:	Date:

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) 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 at: Eric Besendorfer at Dataprivacy@sjbdhs.org. (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.

[SIGNATURE PAGE FOLLOWS]

CONTRACTOR: EDpuzzle, Inc.	
[Signature]	
[Printed Name]	Jaume Bohigas
[Title]	Director of Security and Infrastructure
Date:	

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	**The provision of the Edpuzzle instructional software, accessible at https://edpuzzle.com**
Type of PII that Contractor will receive/access	Check all that apply: x Student PII ☐ APPR Data
Contract Term	Contract Start Date upon signature hereof Contract End Date upon termination of Services
Subcontractor Written Agreement Requirement	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 DPA. (check applicable option) ☐ Contractor will not utilize subcontractors. x Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the DPA, and written request by the EA, Contractor shall:

	• Assist the EA with the download of Student Gradebooks (names, responses, results and grades obtained by students in their assignments), in a standard exportation format such as, but not limited to, .csv or .json. • Thereafter, upon written request by the EA or, in the absence of such written request, upon eighteen (18) months of end-user account inactivity, securely delete and destroy data except for data backups that are part of Contractor's disaster recovery storage system, which may be retained for an additional term of up to three (3) months after termination of services, provided that such backups remain inaccessible to the public and are unable to be used by Contractor in the normal course of its business..
Challenges to Data Accuracy	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 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) X Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Contractor shall implement and maintain reasonable and appropriate technical and organizational security measures to protect the PII with respect to data storage, privacy, from unauthorized access, alteration, disclosure, loss or destruction. Such measures include, but are not limited to: ● 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.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR: EDpuzzle, Inc.	
[Signature]	
[Printed Name]	**Jaume Bohigas**
[Title]	**Director of Security and Infrastructure**
Date:	

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**. While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

DATA SECURITY AND PRIVACY PLAN FOR EDPUZZLE AND SUPPLEMENTAL INFORMATION

The technical and organizational measures provided in this Data Security and Privacy Plan and Supplemental Information (hereinafter, "DSPP") apply to **EDpuzzle, Inc.**, a Delaware corporation (hereinafter, "Edpuzzle"), in the processing of Personally Identifiable Information ("PII") that is the subject matter of the Agreement entered into with _____ ("District") on even date herewith (the "Agreement"), including any underlying applications, platforms, and infrastructure components operated and managed by Edpuzzle in providing its services.

For all aspects not envisaged in the Agreement or this DSPP, Edpuzzle's Terms of Service (http://edpuzzle.com/terms) and Privacy Policy http://edpuzzle.com/privacy) shall apply (jointly the "Service Agreement"), provided such Service Agreement does not contravene the Agreement or this DSPP by any means, in which case the provisions foreseen in the Agreement and this DSPP shall prevail.

1. COMPLIANCE WITH THE LAW

Edpuzzle hereby commits to fully comply with all applicable federal and state laws and regulations on data protection that apply to the processing of PII that is the subject matter of the Agreement. Such laws and regulations may include, without limitation:

a. New York State Education Law §2-D.
b. Family Educational Rights and Privacy Act of 1974 ("FERPA").
c. Children's Online Privacy Protection Act ("COPPA").
d. Children's Internet Protection Act ("CIPA").
e. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), if applicable.

2. DATA PROTECTION

2.1. 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;
b. to provide teachers with analytics on student progress;
c. to help teachers connect with other teachers from the same school or district;
d. to send email updates to teachers, if applicable;
e. to send in-app and push notifications to users, if applicable;
f. to assess the quality of the Service and, if permitted by applicable privacy regulations, improve it;
g. to secure and safeguard personal information and our community;

h. to ensure the Service is used in accordance with the Terms of Service or as required by law, to enhance its security and performance, and monitor and prevent fraudulent activity
i. to access premium features, if applicable; and
j. to comply with applicable laws and regulations.

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 utilizing the Edpuzzle service may provide express consent to receive marketing or commercial communications from Edpuzzle.

2.2. Edpuzzle shall keep strictly confidential all PII that it processes on behalf of District. Edpuzzle shall ensure that any person that it authorizes to process the PII (including Edpuzzle's staff, agents or subcontractors) (each an "authorized person") shall be subject to a strict duty of confidentiality. Edpuzzle shall ensure that only authorized persons will have access to, and process, PII, and that such access and processing shall be limited to the extent strictly necessary to provide the contracted services.

2.3. 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 employment agreements.

2.4. Edpuzzle shall not retain any personal data upon completion of the contracted services unless a student, parent or legal guardian of a student may choose, if and to the extent compatible with the functionality of the service, to independently establish or maintain an electronic account with Edpuzzle after the expiration of the Agreement for the purpose of storing student-generated content.

2.5. Parents, legal guardians, or eligible students may review PII in the student's records and correct erroneous information by contacting their educational institution. Additionally, users may access, correct, update, or delete personal information in their profile by signing into Edpuzzle, accessing their Edpuzzle account, and making the appropriate changes.

3. DATA SECURITY

3.1. Edpuzzle shall implement and maintain reasonable and appropriate technical and organizational security measures to protect the PII with respect to data storage, privacy, from unauthorized access, alteration, disclosure, loss or destruction. Such measures include, but are not limited to:

- 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.

3.2. In the event that PII is no longer needed for the specific purpose for which it was provided, it shall be destroyed as per best practices for data destruction using commercially reasonable care, security procedures and practices.

3.3. Upon the discovery by Edpuzzle of a breach of security that results in the unauthorized release, disclosure, or acquisition of student data, or the suspicion that such a breach may have occurred, Edpuzzle shall promptly notify District of such incident in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of such breach. Edpuzzle will provide District with reasonably requested information about such security breach and status of any remediation and restoration activities; and

3.4. Complaints on how breaches of Student Data are addressed shall be made to Edpuzzle's Data Protection Officer at Av. Pau Casals 16, Pral. 1-A, 08021 Barcelona, Spain or at privacy@edpuzzle.com, as foreseen in Edpuzzle's Privacy Policy.

4. COOPERATION AND INDIVIDUALS' RIGHTS

4.1. To the extent permitted by applicable laws, Edpuzzle shall provide reasonable and timely assistance to District to enable District to respond to:

a. any request from an individual to exercise any of its rights under applicable data protection laws and regulations; and
b. any other correspondence, enquiry or complaint received from an individual, regulator, court or other third party in connection with the processing of Student Data.

4.2. In the event that any such communications are made directly to Edpuzzle, Edpuzzle shall instruct such individual to contact the District directly.

4.3. Parents and legal guardians shall have the right to inspect and review the complete contents of his or her child's processed personal data. Parents and legal guardians that request copies of their children's personal information shall contact District's personnel to that end. At any time, District can refuse to permit Edpuzzle to further collect personal information from its students, and can request deletion of the collected personal information by contacting Edpuzzle at privacy@edpuzzle.com.

5. THIRD-PARTY SERVICE PROVIDERS

5.1. To the extent permitted by law, and as reasonably necessary to provide the Edpuzzle Service to the District, Edpuzzle may provide access to, export, transfer, or otherwise disclose student and/or teacher data to Edpuzzle'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 Edpuzzle under applicable laws and regulations.

5.2. Edpuzzle shall assess the privacy and security policies and practices of third-party service providers to ensure such third-party service providers comply with best industry standards, including, but not limited to, ISO and NIST regulations.

5.3. Edpuzzle only sends PII to third-party service providers that are required to support the service and fully attend Edpuzzle's user needs.

5.4. Edpuzzle's list of third-party service providers is incorporated by reference and is accessible via Edpuzzle's Privacy Policy at https://edpuzzle.com/privacy, which references and links to the current list of third-party service providers maintained at Edpuzzle's Trust Center located at trust.edpuzzle.com.

5.5. In all cases, Edpuzzle shall impose data protection terms on any third-party service provider it appoints, which, at a minimum, meets the requirements set forth in the Agreement.

6. DATA STORAGE

6.1. 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).

6.2. User-generated content (which may or may 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. This would happen if, for example, a user accessed Edpuzzle from Europe and displayed a lesson 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.

7. AGREEMENT EXPIRATION AND DISPOSITION OF DATA

7.1. The Service Agreement shall expire either (a) at District's request upon proactive deletion of user accounts; or (b) in the absence of any specific request or action, upon eighteen (18) months of end-user 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.

7.2. The District will have the ability to download names, responses, results and grades obtained by students in their assignments ("Student Gradebooks") at any point prior to deletion. Except as otherwise provided in applicable laws, return or transfer of data, other than Student Gradebooks, to the District, shall not apply if proven to be incompatible with the Service, technically impossible or to involve a disproportionate effort for Edpuzzle. In such events, and upon written request by the District, Edpuzzle shall proceed to deletion of PII in a manner consistent with the terms of this DSPP, unless prohibited from deletion or required to be retained under state or federal law.

7.3. Without prejudice to the foregoing, Edpuzzle may keep copies and/or backups of data as part of its disaster recovery storage system for an additional term of up to three (3) months after termination of services, provided such data is (a) inaccessible to the public; and (b) unable to be used in the normal course of business by Edpuzzle.

EDpuzzle, Inc.

Signature:

Name: Jaume Bohigas

Title: Director of Security and Infrastructure

Date: