EXHIBIT A

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Morris Central School District Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
Morris Central School District and EDpuzzle, Inc.

1. **Purpose**

(a) Morris Central School District (hereinafter "District") and EDpuzzle, Inc., a Delaware corporation, (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal 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 the District for purposes of providing certain products or services to the District (Vendor's Terms of Service and Privacy Policy, accessible at https://edpuzzle.com/terms and https://edpuzzle.com/privacy, respectively, and hereinafter jointly the "Master Agreement").

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, the Supplemental Information about the Master Agreement between Morris Central School District and Vendor that the District is required by Section 2-d to post on its website and Vendor's Data Privacy and Security Plan.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cyber security Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cyber security (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between Morris Central School District and EDpuzzle, Inc." Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements abiding by data protection obligations consistent with those imposed on Vendor by state and federal law and the Master Agreement, and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor will ensure that any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, have received or will receive training on the federal and state laws governing confidentiality of Protected Data prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District 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 unauthorized release.

(b) Vendor will provide such notification to the District **by contacting Greg Thom directly by email at gthom@morriscsd.org** or by calling (607) 263-6100

(c) Vendor will cooperate with the District and provide as much information as possible directly to Morris Central School District or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, 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 contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, 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 the District 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 the District, Vendor will promptly inform Morris Central School District or his/her designee.

6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) 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 U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cyber security Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data 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 the foregoing, teachers using Vendor's service may provide express consent to receive

commercial communications by enabling (opt-in) or disabling (opt-out) them through their account's settings page.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

EXHIBIT B (CONTINUED)

Bill of Rights for Data Security and Privacy

Morris Central School District

PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records 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.

Third Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of an educational partnership organization that receives student or teacher or Principal data from a school district to carry out is responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;
2. Parents have the right to inspect and review the complete contents of their child's education records. Procedures for reviewing student records can be found in the Board Policy entitled (insert title of FERPA policy);
3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d(5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cyber security Version 1.1 (NIST Cyber security Framework or NIST CSF) is adopted as the standard for data security and privacy;
4. New York state maintains a complete list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaint may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.
6. The District has also established the following procedures for parents to file complaints with the District about breaches or unauthorized releases of student data:
    a. All complaints must be submitted to the District's Data Protection Officer in writing.
    b. Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.
    c. Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

d. Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;
e. The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:
    a. the exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;
    b. how he third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outline in applicable State and federal laws and regulations)e.g., FERPA; Education Law §2-d);
    c. the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District, and whether, when and how the data will be destroyed?;
    d. if and how a parent, student eligible student, teacher or Principal may challenge the accuracy of the student data or teacher or Principal data that is collected;
    e. where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

EXHIBIT C (CONTINUED)

Supplemental Information about a Master Agreement between

Morris Central School District and EDpuzzle, Inc.

Morris Central School District has entered into a Master Agreement with EDpuzzle, Inc., a Delaware corporation, which governs the availability to the District of the following products or services: the Edpuzzle Instructional Software (accessible at www.edpuzzle.com).

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements abiding by applicable data protection, privacy and security requirements consistent with those required of Vendor under the Master Agreement and applicable state and federal law and regulations, including but not limited to Section 2-d of the New York Education Law.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences on the date of the last signature affixed hereto and expires in accordance with the terms outlined in Vendor's attached Data Privacy and Security Plan.
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will, upon written request by the District, securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, except for data backups that are part of Vendor's disaster recovery storage system, which may be kept for and additional term of six (6) months termination of services, provided that (i) such backups remain inaccessible to the public and (ii) Vendor is unable to use such backups in the normal course of its business. If requested by the District, Vendor will assist the District in exporting names, responses, results and grades obtained by students in their assignments ("Student Gradebooks") previously received back to the District for its own use, prior to deletion, in a standard exportation format such as, but not limited to, .csv or .json. In the absence of a written request by the District, Vendor will delete all Protected Data, with the exception of the aforementioned data backups, upon eighteen (18) months of end-user account inactivity.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will, upon written request by the District, cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- 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. Upon written request, Vendor will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.
- Vendor may use De-identified data for purposes of research, improvement of Vendor's product or services, and/or development of new products and services. In no event shall Vendor or any of its subcontractors or assignees re-identify or try to re-identify any De-identified data or use De-identified

data in combination with other data elements possessed by Vendor or any third-party affiliate, posing risk of re-identification.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection. Notwithstanding the foregoing, user-generated content (which may or may not include Protected Data) may be temporarily copied and stored in other countries in order for Vendor 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.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

Agreement and Signature

By signing below, you agree:

- To comply with the terms contained in the Supplemental Information Master Agreement
- To comply with the terms of Morris Central Schools Parents' Bill of Rights for Data Privacy and Security (applicable to Third-Party Contractors subject to New York Education Law § 2-d only)

BY THE VENDOR:

EDpuzzle, Inc.	Edpuzzle Instructional Software	
Company Name	**Product Name**	
Jaume Bohigas	Jaume Bohigas	February 19, 2
Name (Print)	**Signature**	**Date**

BY THE DISTRICT:

Morris Central School District		
District Name		
Greg Thom	Greg Thom Greg Thom (Feb 26, 2024 09:51 EST)	2/26/2024
Name (Print)	**Signature**	**Date**

Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

Morris Central School District and the Vendor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and Morris Central School District's Data Security and Privacy Policy;

3. The Parties agree that the Morris Central School District Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Vendor shall comply with its terms;

4. The Vendor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Vendor agrees that any officers or employees of the Vendor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Vendor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes; notwithstanding the foregoing, teachers using Vendor's service may give express consent to receive commercial communications;
    c. except for authorized representatives of the Vendor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
    e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure 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;
    f. adopt technology, safeguards and practices that align with the NIST Cyber security Framework;
    g. impose terms consistent with those of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

EDpuzzle, Inc.	Edpuzzle Instructional Software	
Company Name	**Product Name**	
Jaume Bohigas	Jaume Bohigas	February 19,
Name (Print)	**Signature**	**Date**

Exhibit D (continued)

Vendor's Data Privacy and Security Plan

DATA PRIVACY AND SECURITY PLAN FOR EDPUZZLE AND SUPPLEMENTAL INFORMATION

The technical and organizational measures provided in this Data Privacy and Security Plan and Supplemental Information (hereinafter, "DPSP") 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 Morris Central School District ("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 DPSP, 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 DPSP by any means, in which case the provisions foreseen in the Agreement and this DPSP 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 improve it;**
g) **to secure and safeguard personal information of other data subjects;**
h) **to access premium features, if applicable;**
i) **to comply with all applicable laws and regulations 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 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:

(1) **any request from an individual to exercise any of its rights under applicable data protection laws and regulations; and**
(2) **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 maintained online and may be found in Edpuzzle's Privacy Policy.

5.5. In all cases, Edpuzzle shall impose the data protection terms on any third-party service provider it appoints that at a minimum meets the requirements provided for by 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 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 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.

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, 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.

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 the 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 DPSP, 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 six (6) 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.