

**AGREEMENT  
REGARDING DATA SECURITY AND PRIVACY**

This Agreement is made as of the date of the last signature affixed hereto, by and between the East Rockaway Union Free School District (“District”) and EDPuzzle, Inc. (“Contractor”).

WHEREAS, the District has entered into a contract or other written agreement, as defined in Part 121 of the Commissioner’s Regulations, with Contractor for certain services or products, a copy of which can be found at [www.edpuzzle.com/terms](http://www.edpuzzle.com/terms) and [www.edpuzzle.com/privacy](http://www.edpuzzle.com/privacy); and

WHEREAS, Contractor is a third-party contractor as defined in Part 121 of the Commissioner’s Regulations, that will receive student data or teacher or principal data from the District pursuant to said contract or other written agreement for purposes of providing services to the District; and

WHEREAS, the parties agree that if any provision of this Agreement conflicts with a provision of said contract or other written agreement, the provision as set forth in this Agreement shall supersede and prevail over said other provision;

NOW, THEREFORE, in consideration of the mutual covenants, conditions and agreements contained herein, and for other good and valuable consideration, including the above-referenced contract or other written agreement, the Contractor and the District hereby agree as follows:

A. The Contractor shall comply with all District policies and state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the District’s Parents’ Bill of Rights and Supplemental Information, annexed hereto and incorporated herein as Attachment “A”.

B. The Contractor may receive personally identifiable information from student records (“Education Records”) and/or personally identifiable information from annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release pursuant to Education Law § 3012-c and 3012-d (collectively, “PII Data”). The Contractor shall, therefore, comply with the following provisions in order to maintain the security and confidentiality of personally identifiable information:

- (i) adopt technologies, safeguards and practices in alignment with the NSIT Cybersecurity Framework;
- (ii) comply with the school district’s data security and privacy policy;
- (iii) limit the Contractor’s internal access to Education Records to individuals with legitimate educational interests;
- (iv) use PII Data only for the purposes explicitly authorized by this Agreement and not for any other purpose;
- (v) not disclose any personally identifiable information from PII Data to any other party without prior written consent, unless disclosure is required by statute or

court order and written notice is given to the District (notice is not required if it is expressly prohibited by a statute or court order);

- (vi) maintain reasonable safeguards to maintain confidentiality of personally identifiable information in PII Data;
- (vii) use legally mandated encryption technology<sup>1</sup> to protect data from unauthorized disclosure while the data is in motion or in the contractor's custody; and
- (viii) not sell, use or disclose student, teacher or principal personally identifiable information for any marketing or commercial purpose; nevertheless, teachers using Contractor's service may provide express consent to receive marketing or commercial communications.

C. The Contractor represents and warrants that its contract or written agreement with the District includes the Contractor's data security and privacy plan that is acceptable to the District, a copy of which is attached hereto and incorporated herein as Attachment "B". The Contractor's data security and privacy plan shall, at a minimum:

- (i) outline how the Contractor will implement State and federal data security and privacy contract requirements for the life of the contract and is consistent with the school district's data security and privacy policy;
- (ii) specify administrative, operational and technical safeguards the third-party contractor will use to protect personally identifiable information;
- (iii) show that it complies with requirements of §121.3(c) of the Commissioner's Regulations;
- (iv) specify how the third-party contractor's employees and any assignees with access to student data, or teacher or principal data receive or will receive training on relevant confidentiality laws, before receiving access to such data;
- (v) specify if the third-party contractor will use subcontractors and how it will ensure personally identifiable information is protected;
- (vi) specify an action plan for handling any breach or unauthorized disclosure of personally identifiable information and promptly notify the school district of any breach or unauthorized disclosure; and
- (vii) describe whether, how and when data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated.

D. The Contractor must notify the District of any breach of security resulting in an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employee's, assignees or subcontractors. This notification must be made in the most expedient way possible and without delay. In addition, the Contractor must notify the District of the breach of security in writing. This written notification must be sent by the Contractor in the most expedient way possible and without unreasonable delay, and not later than seven (7) calendar days after discovery of the breach of security resulting in an unauthorized release of personally identifiable information from PII Data, to the designated

---

<sup>1</sup> Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.

District representative and either personally delivered or sent by nationally recognized overnight carrier to the District. In the case of an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employees, assignees or subcontractors, the Contractor must reimburse the District for all the District's costs associated with the District's obligation to notify the State's chief privacy officer, parents, students, teachers and/or principals of the unauthorized release.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

DISTRICT

CONTRACTOR

BY: Lee Ariz

BY: Jordi Gonzalez

DATE: 12/31/2020

DATE: 12/30/2020

## **PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY**

The East Rockaway Union Free 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 education records from unauthorized access or disclosure in accordance with State and federal law, and establishes the following parental bill of rights:

1. Students' personally identifiable information will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and federal Law;
2. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third-party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
3. Parents have the right to inspect and review the complete contents of their child's education record;
4. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
5. A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov.data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234;
6. Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Privacy Officer at 516-887-8300 Ext. 440 or by mail to the Data Privacy Officer, East Rockaway School District, 443 Ocean Avenue, East Rockaway, NY 11518. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov.data-privacy-security>, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to [privacy@mail.nysed.gov](mailto:privacy@mail.nysed.gov) or by telephone at 5178-474-0937.
7. Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's personally identifiable information occurs;

8. Parents can expect that educational agency workers who handle personally identifiable information will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect personally identifiable information;
9. In the event that the District engages a third party provider to provide, deliver or facilitate student educational services, the contractor or subcontractors will be obligated to adhere to the District's data security and privacy policy and with State and federal laws to safeguard students' personally identifiable information, as well as to this Bill of Rights and required supplemental information for each contract.
10. This Parents' Bill of Rights will be included with every contract or other written agreement entered into by the District with a third-party contractor if the contractor will receive student data or teacher or principal data. The Bill of Rights shall also be supplemented to include information about each contract or other written agreement that the District enters into with a third-party contractor receiving student data or teacher or principal data, including: the exclusive purpose(s) for which PII Data will be used; how the contractor will ensure confidentiality and data protection and security requirements; the duration and date of expiration of the contract and what happens to PII Data upon the expiration of the contract; if and how the accuracy of PII Data collected can be challenged; where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and how PII Data will be protected using encryption while in motion and at rest.
11. Parents can request information about third party contractors by contacting the Data Privacy Officer at 516-887-8300 Ext. 440 or by mail at 443 Ocean Avenue, East Rockaway, NY 11518 or can access the information on the district's website <http://eastrockawayschools.org/departments/technology>
12. This Parents' Bill of Rights and supplemental information for contracts with third-party contractors shall be posted the district website at the following link: <http://eastrockawayschools.org/departments/technology>

\* \* \*

**PARENTS' BILL OF RIGHTS FOR STUDENT  
DATA PRIVACY AND SECURITY  
THIRD PARTY CONTRACTOR SUPPLEMENT**

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

(1) The student data or teacher or principal data (collectively, "PII Data") received by the Contractor will be used exclusively for the provision of the "Edpuzzle Service".

Contractor and its agents, employees and subcontractors, if any, shall use PII Data solely for the purpose of providing services as set forth in the parties' contract or other written agreement. Contractor and its agents, employees and subcontractors will not use PII Data for any other purposes. Any Data received by or by Contractor or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes. Notwithstanding the aforementioned, teachers using Contractor's service may provide express consent to receive marketing or commercial communications.

(2) The Contractor will ensure the confidentiality of PII Data that is shared with subcontractors or other persons or entities as follows:

In the event that Contractor subcontracts with an outside entity or individual in order to fulfill its obligations to the District, Contractor ensures that it will only share PII Data with such subcontractors if those subcontractors are contractually bound to observe obligations to maintain data privacy and security consistent with those required of Contractor pursuant to the Agreement. Contractor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII Data in its custody consistent with the data protection and security requirements of district policy, and state and federal law and regulations, as further outlined in Contractor's [Privacy Policy](#) and the attached Data Security and Privacy Plan.

(3) The duration of Contractor's services begins on the date of signature hereof and ends upon deletion of end-user accounts, as set forth in the parties' contract or other written agreement. Once the contractor has completed its service to the district, records containing PII Data received by the Contractor will be disposed of as follows:

All PII Data will be disposed of in accordance with the instructions of the District, and will be: (a) to the extent feasible, delivered to the District, (b) de-identified and/or (c) deleted from Contractor's computer systems and destroyed, except for backups of data that are part of Contractor's disaster recovery storage system, which may be retained for a term up to thirteen (13) months since termination of the service. Contractor will provide written confirmation of such disposition to the District, upon written request.

(4) A parent, student, teacher or principal can challenge the accuracy of PII Data

received by the Contractor as follows:

In the event that a parent or eligible student wishes to challenge the accuracy of PII Data concerning that student that is maintained by Contractor or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Contractor is notified of the outcome of any such errors made by Contractor, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The District or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Contractor or its subcontractors.

(5) The following is how PII Data will be stored and what security protections will be taken by the Contractor:

All Data in Contractor's possession will be securely stored in externalized databases that are currently being provided by MongoDB Atlas ([security compliance information](#)), and simultaneously hosted on Amazon Web Services ([security and compliance information](#)) in North Virginia (United States).. Contractor represents that the following security protections, including encryption where applicable, will be in place to ensure that PII Data is protected:

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls
- 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.



**EDpuzzle, Inc.**  
833 Market St. (Suite 427)  
San Francisco, CA 94103  
[privacy@edpuzzle.com](mailto:privacy@edpuzzle.com)

## **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. (hereinafter, “Edpuzzle”) in the processing of Personally Identifiable Information (“PII”) that is the subject matter of the Agreement entered into with East Rockaway Union Free School District (“District”) on 12 / 30 / 2020 (the “Agreement”), including any underlying applications, platforms, and infrastructure components operated and managed by Edpuzzle in providing its services.

### **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 improving the Services and for the following limited purposes:

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

Edpuzzle shall not use PII for any purposes other than those authorized pursuant to the Agreement and may not use PII for any targeted advertising or other commercial uses.

**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 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 personally identifiable information 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:

- Pseudonymisation and encryption of PII.
- 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, including any copies of the personal data that may reside in system backups, temporary files, or other storage media, it shall be destroyed as per best practices for data destruction or returned to District 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:

- (a) promptly notify District of such incident. Edpuzzle will provide District with reasonably requested information about such security breach and status of any remediation and restoration activities; and

- (b) Complaints on how breaches of Student Data are addressed shall be made to Edpuzzle's Data Protection Officer at Av. Pau Casals 16, Ppal. 2-B, 08021 Barcelona, Spain or at [privacy@edpuzzle.com](mailto: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 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](mailto:privacy@edpuzzle.com).

#### **5. THIRD-PARTY SERVICE PROVIDERS**

**5.1.** Edpuzzle assesses the privacy and security policies and practices of third-party service providers. To that effect, Edpuzzle hereby declares to have agreements in place with such service providers to ensure that they are capable of complying with Edpuzzle's Privacy Policies and thus comply with industry standards on data protection.

**5.2.** Edpuzzle only sends personal identifiable information to third-party services that are required to support the service and fully attend Edpuzzle's user needs.

**5.3.** Edpuzzle's list of third-party service providers is maintained online and may be found in Edpuzzle's [Privacy Policy](#).

**5.4.** 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 ([security compliance information](#)), and simultaneously hosted on Amazon Web Services ([security and compliance information](#)) in North 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.

**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 personally identifiable information 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, provided such data is (a) inaccessible to the public; (b) unable to be used in the normal course of business by the company; and (c) deleted after a maximum term of thirteen (13) months since the creation of said copies and/or backups. In case such copies and/or backups are used by Edpuzzle to repopulate accessible data following a disaster recovery, the District shall be entitled to demand from the company the immediate deletion of said copies and/or backups, by sending a written request at [privacy@edpuzzle.com](mailto:privacy@edpuzzle.com).

## **8. EDPuzzle's TERMS OF SERVICE AND PRIVACY POLICY**

For all aspects not envisaged in this Data Security and Privacy Plan, Edpuzzle shall subject student data processing to its own [Terms of Service](#) and [Privacy Policy](#), to the extent such documents do not contravene the Agreement by any means, in which case the provisions foreseen in the Agreement shall prevail.

<b>TITLE</b>	East Rockaway SD - NY_DPA
<b>FILE NAME</b>	East Rockaway SD - NY_DPA.pdf
<b>DOCUMENT ID</b>	e64a8c712c778a4643978b27e4e59faaf25537bd
<b>AUDIT TRAIL DATE FORMAT</b>	MM / DD / YYYY
<b>STATUS</b>	● Completed

## Document History



SENT

**12 / 09 / 2020**  
 17:15:23 UTC+1

Sent for signature to Jordi González (jordi@edpuzzle.com)  
 from julia@edpuzzle.com  
 IP: 80.30.124.218



VIEWED

**12 / 30 / 2020**  
 11:17:17 UTC+1

Viewed by Jordi González (jordi@edpuzzle.com)  
 IP: 2.152.162.145



SIGNED

**12 / 30 / 2020**  
 12:02:50 UTC+1

Signed by Jordi González (jordi@edpuzzle.com)  
 IP: 2.152.162.145



COMPLETED

**12 / 30 / 2020**  
 12:02:50 UTC+1

The document has been completed.