Alexandria Central School
Home of the Purple Ghosts

34 Bolton Avenue, Alexandria Bay, New York 13607 Phone: 315-482-9971 Fax: 315-482-9973

CONTRACT ADDENDUM
Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Alexandria Central School District ("DISTRICT") and EDpuzzle Inc. ("Vendor") are parties to a contract made on the same date of the signature hereof ("Effective date") governing the terms under which DISTRICT accesses, and Vendor provides, the Edpuzzle educational software ("Product") (Vendor's Terms of Service and Privacy Policy, hereinafter "the underlying contract"). DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.

2.2 "Vendor" means EDpuzzle, Inc. .

2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.

2.4 "DISTRICT" means the School District.

2.5 "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6 "Student" means any person attending or seeking to enroll in an educational agency.

2.7 "Eligible Student" means a student eighteen years or older.

2.8 "Subcontractor" shall mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9 "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the DISTRICT Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; and shall not be used by Vendor or its Assignees to market products or services to students. Notwithstanding the foregoing, teachers using the service may receive commercial communications if express consent is given to that end.

7. Ownership and Location of Protected Information

7.1 Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2 DISTRICT shall have access to the DISTRICT's Protected Information at all times through the term of this Contract.

DISTRICT shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor. Except as otherwise provided in applicable laws, transfer of data shall not apply if proven to be incompatible with the Service, technically impossible or to involve a disproportionate effort for Vendor.

7.3 All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. 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. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS, Canada or the Economic European Area (EEA). All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS, Canada or the EEA.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be a "Subcontractor" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe obligations to maintain the privacy and security of Protected Information consistent with those that are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1 The expiration date of this Contract is defined by the underlying contract.

10.2 Upon expiration of this Contract without a successor agreement in place, Vendor shall, upon written request by DISTRICT, assist DISTRICT in exporting, to the extent feasible, Protected Information previously received from, or then owned by, DISTRICT.

10.3 Vendor shall thereafter, and upon written request by DISTRICT, securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities, except for backups of data that are part of Vendor's disaster recovery storage system, and which may be retained for an additional term of thirteen (13) months since termination of the services. This Addendum shall continue to apply for as long as the Vendor retains possession over Protected Information.

10.4 Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities, except for backups of data that are part of Vendor's disaster recovery storage system, in the terms outlined in section 10.3 above.

10.5 To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6 Upon request, Vendor will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1 In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2 Vendor will cooperate with DISTRICT in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1 Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2 Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy (Attachment B);

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and

i. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this c ontract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the DISTRICT unless (i) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will 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 U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay **but no more than seven (7) calendar days** after the discovery of the breach; and

13.7 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

For Alexandria Central School District

Date: 11/30/2020

For EDpuzzle Inc.

Julia Trius

Date: 12 / 02 / 2020

ATTACHMENT A – PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
Alexandria Central School District: Parents Bill of Rights for Data Privacy and Security

For Alexandria Central School District

Date: 11/30/2020

For EDpuzzle Inc.

Julia Trius

Date: 12 / 02 / 2020

Supplemental Information About This Contract

CONTRACTOR	EDpuzzle Inc.
PRODUCT	Edpuzzle instructional software
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe obligations to maintain the privacy and security of Protected Information consistent with those that are required of Vendor under this Contract and all applicable New York State and federal laws.
DATA DESTRUCTION INFORMATION	The agreement expires August 31, 2021 , unless either party gives notice to terminate. Upon expiration of this Contract without a successor agreement in place and written request by the DISTRICT, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT, to the extent such export is feasible. Vendor shall thereafter, upon request by the DISTRICT, securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities. Without prejudice to any of the foregoing, Vendor may retain backups of data for a term up to thirteen (13) months since termination of the agreement and/or the service, provided the terms of the agreement and this addendum shall continue to apply so long the Vendor retains Protected Information in its possession.
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Education Rights and Privacy Act.
SECURITY PRACTICES	The data is stored in the continental United States (CONUS) or Canada. 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 Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will 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 U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).

ATTACHMENT B – DISTRICT POLICY

https://docs.google.com/document/d/1bL4-Pi2rXvSpPRQ187ca2cDYDnBMD8PL6hIX-8RPUYM/edit?usp=sharing

Attachment C – Vendor's Data Security and Privacy Plan

The DISTRICT Parents Bill of Rights for Data Privacy Security, a signed copy of which is included as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

edpuzzle

EDpuzzle, Inc.
833 Market St. (Suite 427)
San Francisco, CA 94103
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 Alexandria Central School ("District") on 12 / 02 / 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, 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.

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 DSPS, 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.

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.

HELLOSIGN

Audit trail

TITLE	Alexandria_CS - NY - DPA
FILE NAME	2D Contract Adden... EDPuzzle ACS.pdf
DOCUMENT ID	b4c22e2763c96cd196339d63d0ed7236ca9adaf2
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document history

SENT	**12** / **01** / **2020** 10:47:46 UTC	Sent for signature to Julia Trius (julia@edpuzzle.com) from jan@edpuzzle.com IP: 88.9.86.180
VIEWED	**12** / **02** / **2020** 09:25:14 UTC	Viewed by Julia Trius (julia@edpuzzle.com) IP: 93.176.141.206
SIGNED	**12** / **02** / **2020** 10:35:52 UTC	Signed by Julia Trius (julia@edpuzzle.com) IP: 93.176.141.206
COMPLETED	**12** / **02** / **2020** 10:35:52 UTC	The document has been completed.