Data Security and Privacy Policy

Definitions:

1. Protected Data means personally identifiable data 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.

Requirements:

1. Publication: This policy shall be published on the District's website and notice of the policy provided to all officers and employees of the District.
2. The District shall provide the data protection as well as the protection of parent and eligible student's rights and rights to challenge the accuracy of such data required by FERPA (20 USC §1232g), IDEA (20 USC §1400 et. seq.) and any implementing regulations.
3. The District hereby adopts the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) in accordance with the Commissioner's Regulations.
4. Every contract or other written agreement with a third party contractor under which the third party contractor will receive protected student data or teacher or Principal data shall include a data security and privacy plan that outlines how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with this policy.
5. Nothing contained in this policy or the District's Data Security and Privacy Plan shall be construed as creating a private right of action against the District.
6. Every use and disclosure of personally identifiable information, as defined by FERPA, shall be for the benefit of students and the educational agency. Examples of such benefit are provided in implementing regulations.
7. The District shall not sell or disclose for marketing or commercial purposes any Protected Data, or facilitate its use of disclosure by any other party for any marketing or commercial purpose, or permit another party to do so.
8. The District shall take steps to minimize its collection, process and transmission of Protected Data.
9. Except as required by law or in the case of enrollment data, the District shall not report to NYSED Juvenile Delinquency records, criminal records, medical health records, or student biometric information.
10. All contracts with vendors that have access to Protected Data shall comply with NIST Cybersecurity Framework.

Adopted 6/1/20

Parents Bill of Rights Relating to Student Data

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 personal 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 the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its 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 not 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 record. Procedures for reviewing student records can be found in the Board Policy entitled: **#26 Policies and Procedures and Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information** – *Section 1 – Legally Mandated Policies*;

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 Cybersecurity Version 1.1 (NIST Cybersecurity 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, NY 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Records Access Officer, Joseph Gugino, Oxford Academy and Central School District, PO Box 192, Oxford, NY 13830;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

- 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;

- Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District hall 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;

- The District will require complaints to be submitted in writing;

- 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:

- 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;
- How the 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 outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);
- 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);
- If an 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;
- 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.

8. 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.

Agreement and Signature

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

Company Name EDPUZZLE, INC. Product Name EDPUZZLE

Printed Name JORDI GONZALEZ Signature Jordi Gonzalez Date 10 / 26 / 2020

Adopted 5/9/16

Amended 6/1/20

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

Oxford Academy and Central School and the Third-Party Contractor 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 the Oxford Academy and Central School's Data Security and Privacy Policy;

3. The Parties agree that the Oxford Academy and Central School's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

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

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, 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 Third-Party Contractor agrees to make sure that, prior to disclosing any Protected Information to any assignee, such assignee complies with any federal and state law governing confidentiality of such information.

7. The Third-Party Contractor 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. Without prejudice to the foregoing, users of "teacher accounts" may receive marketing communication if express consent has been given for that purpose. Such communications may be enabled or disabled at any time, through the "teacher account's" settings page;
    c. except for authorized representatives of the Third-Party Contractor, including subcontractors supporting Third-party Contractor's business, and 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 Cybersecurity Framework;

g. impose obligations consistent with all the terms of this rider in writing where the Third-Party Contractor 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:

Company Name EDPUZZLE, INC. Product Name EDPUZZLE

Printed Name JORDI GONZALEZ Signature Jordi Gonzalez Date 10 / 26 / 2020 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 Oxford Academy and Central School ("District") on 10 / 26 / 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 Data/will be used by Edpuzzle for improving the Services and for the following limited purposes:
Teacher Data

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 the 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 Policy does not contravene the Agreement by any means, in which case the provisions foreseen in the Agreement shall prevail.

HELLOSIGN

Audit Trail

TITLE	Oxford Academy CS - NY_DPA
FILE NAME	Oxford academy fi...iewed version.pdf
DOCUMENT ID	f98aefdc0d9441ca2235aba8376e76b045b4fc19
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document History

SENT	**10** / **08** / **2020** 11:09:54 UTC+1	Sent for signature to Jordi González (jordi@edpuzzle.com) from julia@edpuzzle.com IP: 81.34.57.22
VIEWED	**10** / **26** / **2020** 16:42:46 UTC+1	Viewed by Jordi González (jordi@edpuzzle.com) IP: 2.152.162.145
SIGNED	**10** / **26** / **2020** 17:07:12 UTC+1	Signed by Jordi González (jordi@edpuzzle.com) IP: 2.152.162.145
COMPLETED	**10** / **26** / **2020** 17:07:12 UTC+1	The document has been completed.