D. Parents' Bill of Rights and Supplemental Information

1. Parents' Bill of Rights

Vendor acknowledges and agrees that the District's Parents' Bill of Rights as set forth herein and as posted on the District's website is incorporated into these Terms and Conditions.

The North Collins Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

2) Parents have the right to inspect and review the complete contents of their child's education record.

3) State and federal laws protect the confidentiality of personally identifiable information, and 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.

4) A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/student-data-privacy or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 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. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy

2. Supplemental Information

i. The exclusive purpose for which Protected Data will be used is for the provision of the "Edpuzzle Service" (www.edpuzzle.com) under a school district subscription. Vendor will not use the Protected Data for any other purposes not explicitly authorized herein or within the Master Agreement.

ii. In the event that Vendor engages subcontractors or other authorized persons or entities ("Subcontractors") to perform one or more of its obligations under the Master Agreement (including hosting of the Protected Data), Vendor will require Subcontractors to execute legally binding agreements acknowledging and agreeing to comply with data protection, privacy and security requirements consistent with those required of Vendor under the Master Agreement, these Terms and Conditions, and applicable state and federal law and regulations.

iii. The Master Agreement commences on the same date of signature hereof and expires on June 30, 2023. Upon written request by the District and expiration of the Master Agreement without renewal, or upon written request by the District and termination of the Master Agreement prior to its expiration, Vendor will 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. If requested by the District, Vendor will assist the District in exporting Student Gradebooks[1] previously received back to the District for its own use, prior to deletion, in a standard electronic legible format. 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 Vendor.

iv. In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any Subcontractors will retain any Protected Data, copies, summaries or extracts of the Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or Subcontractors will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full. Vendor agrees that in no event shall Vendor or its assignees or Subcontractors re-identify or attempt to re-identify any de-identified Protected Data, nor shall they use de-identified Protected Data with other data elements posing risk of re-identification. Vendor may use de-identified data solely for the purposes of research, to improve the service or develop new products or services.

During the term of the Agreement, Vendor 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.

v. Parents or eligible students can challenge the accuracy of any Protected Data in accordance with the District's 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

[1] Names, responses, results and grades obtained by students in their Edpuzzle assignments.

APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

vi. Any Protected Data will be stored on systems maintained by Vendor, or Subcontractor(s) under the direct control of Vendor, in a secure data center facility. The measures that Vendor (and, if applicable, Subcontractor(s)) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, "NIST Cybersecurity Framework" (Version 1.1) and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

vii. Vendor (and, if applicable, Subcontractor(s)) will use encryption to protect Protected Data in its custody while in motion and while at rest, using a technology or methodology specified or permitted 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.

3. Posting

In accordance with Section 2-d, the District will publish the Parents' Bill of Rights and Supplemental Information from these Terms and Conditions on its website. The District may redact the Parents' Bill of Rights and Supplemental Information to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

IN WITNESS WHEREOF, the Parties have indicated their acceptance of these Terms and Conditions including the Parents' Bill of Rights and Supplemental Information by their signatures below on the dates indicated.

BY THE VENDOR:

JORD GONZALEZ
Name (Print)

Jordi Gonzalez
Signature

PRODUCT MANAGER, CO-FOUNDER
Title

11 / 16 / 2020
Date

BY THE DISTRICT:

SCOTT TAYLOR
Name (Print)

Signature

SUPERINTENDENT
Title

10-30-20
Date