Addendum "A"

DATA PRIVACY PLAN AND PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("PII") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy.

As such, [EXPLORELEARNING, LLC] agrees that the following terms shall be incorporated into the contract for services ("the Contract") and it shall adhere to the following:

1. The Contactor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here:

   ExploreLearning's complete Privacy Policy can be found at:

   a. *Gizmos*: www.explorelearning.com/privacy
   b. *Reflex*: www.reflexmath.com/privacy
   c. *Science4Us*: https://www.science4us.com/privacy-policy/

2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.

3. The exclusive purposes for which the student data or teacher or principal data will be used under the contract are set forth in the Terms of Service with ExploreLearning.

4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:

   a. PII data will be protected using encryption while in motion and at rest by [ENTER HOW].

   ExploreLearning uses secure encryption technology (secure socket connection) for all sensitive data transmitted on Gizmos, Reflex, and Science4Us. Information is encrypted at rest and also in transit between our data center and client machines (using HTTPS). Our certificates are from Entrust. Data is encrypted at REST at AES 128 or higher. All of our administrative controls are behind our firewall (only accessible from within our VPS) and also require username/password access.

   b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored by [*ExploreLearning operates and maintains our systems in good working order and provides secure, restricted access to our systems. We provide secure storage for all data stored on our systems. We are FERPA and COPPA compliant and work with an independent company to assess our systems' compliance each year. Gizmos collects a minimal amount of information. Customer data is stored in our*

databases, which are maintained in dedicated servers housed in our secure Texas data center. Data that is collected is by virtue of student interactions with Gizmos is exchanged via encrypted channels using HTTPS. Reflex collects student roster and response data related to their performance in the system. This data is stored in our databases, which are maintained in dedicated servers housed in our secure Dallas data center. Data that is collected is by virtue of student interactions with Reflex is exchanged via encrypted channels using HTTPS. Science4Us collects a minimal amount of information. Customer data is stored in our databases, which are maintained in dedicated servers hosted in the Microsoft Azure Cloud. Data that is collected is by virtue of student interactions with Science4Us is exchanged via encrypted channels using HTTPS.]. The security of this data will be ensured by [*See the privacy policies for more information*.].

c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows: [*Background checks completed on personnel with access to servers, applications and customer data. Data and servers are kept in secure facilities onsite with authorized personnel with entry fobs. Data at rest is encrypted with AES 256 or XTS-AES 128.*]

5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.

   a. By initialing here ___JMG_____ Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.

   b. [*All Employees and contractors are subject to background checks and company privacy policies and security training*.]

6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII will abide by all applicable data protection and security requirements, including, but not limited to those outlined in applicable laws and regulations (e.g., FERPA, Education Law Section 2-d). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows: [*All employees with access to pupil records have received annual FERPA Compliance training*]

7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Specifically, [*School data is deleted either within a reasonable time-frame after contract expiration or on request from a customer*.]

9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.

10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII. [DESCRIBE – below are minimum requirements]

    In the case of an unauthorized disclosure of student data (such as a data breach), any known security violations will be recorded in the ExploreLearning's help desk system along with the remediation actions taken. Each known violation will be communicated to all affected school district personnel who need to know, and this communication will occur within 24 hours of the awareness of the violation. ExploreLearning will collaborate closely and privately with affected teachers and administrators with full transparency of the facts pertaining to each incident.

    a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email.

    b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.

    c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.

11. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

The District shall publish this contract addendum on its website.

Julia M Given

Julia M Given
VP Finance

6/12/20
Date