DS

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the "Agreement") is made and entered by and between **Discovery Education, Inc.** ("Vendor"), address: **4350 Congress St, Ste 700, Charlotte, NC 28209** and Delaware Academy Central School District at Delhi ("Customer"), 2 Sheldon Drive, Delhi, NY 13753 on the date signed by the Vendor.

WHEREAS, the Vendor will receive student data and/or teacher or principal data ("Protected Data") that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from Customer for purposes of providing online digital science curriculum at mysteryscience.com and mysterydoug.com websites to Customer and

WHEREAS, both Customer and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

NOW THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement the parties hereto mutually agree as follows:

1. Confidentiality

a. Vendor, its employees, and/or agents agree that all information obtained from Customer's employees or students is deemed confidential information in accordance with the Contract.

b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with applicable federal and state law and that any information obtained will not be revealed to any persons, firms or organizations to the extent permissible by law.

2. Data Protections and Internal Controls

a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by Customer that directly relate to a student(s) (hereinafter referred to as "education record").

b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with applicable state data security and privacy standards for all personally identifiable information from education records, and it shall:

1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and

2. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

3. To use encryption technology to protect Protected Data in its custody while in motion or at rest. Customer agrees that these encryption methods meet the standards described in 8 NYCRR 121. More details of Vendor's security practices can be found in the (link to policy) https://www.discoveryeducation.com/data-%20protection-addendum/.

3. Data Security and Privacy Plan

a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from Customer, the policies and procedures of which can be found at https://www.discoveryeducation.com/data-%20protection-addendum/. which may be updated from time to time.

4. Notice of Breach and Unauthorized Release

a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:

1. Promptly notify Customer in the most expedient way possible and without unreasonable delay after Vendor has discovered or been informed of the breach or authorized release.

2. Advise Customer as to the nature of the breach and steps Vendor has taken to minimize said breach.

b. In the case of required notification to a parent or eligible student, the Vendor shall:

1. Promptly reimburse Customer for the actual costs of such notification.

c. Vendor will cooperate with Customer and provide as much information as is legally possible directly to Customer about the incident, including but not limited to:

1. The description of the incident;

2. The date of the incident;

3. The date Vendor discovered or was informed of the incident;

4. A description of the types of Protected Data involved;

5. An estimate of the number of records affected;

6. The schools within Customer's purview that are affected;

7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data; and

8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

e. Vendor acknowledges that upon initial notification from Vendor, Customer, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by Customer or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Customer, Vendor will promptly inform Customer of the same.

5. Vendor Information

Vendor understands that as part of Customer's obligations under New York Education Law Section 2-d, Vendor is responsible for providing Customer with Vendor information (see Vendor Information for Data Privacy and Security) to include:

a. Exclusive purposes for which the student data will be used;

b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;

c. That student data will be destroyed upon expiration of the Agreement;

d. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and

e. Where the student 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, including whether such data will be encrypted.

6. Termination or Expiration of Contract and/or Agreement

a. Upon termination of the Agreement, and upon request, Vendor shall destroy all confidential information obtained in connection with the services provided therein and/or student data to the extent legally permissible. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement.

b. If requested by Customer, Vendor will assist Customer in exporting all Protected Data previously received back to Customer for its own use, prior to deletion, in such formats as may be reasonably requested by Customer.

c. In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with Customer necessary to transition Protected Data to the successor Vendor prior to deletion.

d. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever to the extent legally permissible. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Customer with a certification from an appropriate officer that these requirements have been satisfied in full.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Customer 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, Customer 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/data privacysecurity/student-data-inventory 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 submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to Customer by contacting Kelly Pinter directly at kpinter@delhischools.org, or by calling (607) 746- 1315. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: http://www.nysed.gov/data privacysecurity/report-improper-disclosure

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION DETAILS

Vendor: Discovery Education, Inc.

Collects: ☐ XStudent Data ☐ XTeacher or Principal Data ☐ Does not collect either

Educational agencies including Delaware Academy School District are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

Part 1: Exclusive Purposes for Data Use
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor: **The services provided are access by the School District's teachers and staff to the online digital science curriculum at mysteryscience.com and mysterydoug.com websites.**
Part 2: Third-part Contractor Oversight Details – Select the appropriate option below.
☐ This contract has no third-party contractors. ☐ X This contract has third-party contractors. If this option is checked, please lit how Vendor will ensure that the any other entities with which it shares protected data will comply with the data protection and security provisions of the law and this agreement. **The Contractor will ensure that its personnel and subcontractors that access the student data are informed of the confidential nature of the student data and are bound by appropriate obligations of confidentiality or are under an appropriate statutory obligation of confidentiality. The Contractor will take all reasonable steps and to ensure the reliability of Contractor's personnel and subcontractors that access student data.**
Part 3: Agreement Lifecycle Practices
The Agreement expires thirty-six (36) months from the effective date. Upon expiration, protected data will be deleted by the contractor, via shredding, mass deletion, and upon request, may be exported for use by the district before deletion.
Part 4: Student Educational Records / Improper Disclosure

A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website.

B. A report of improper disclosure must be made to Customer as soon as improper disclosure is identified.

Part 5: Security Practices

Please describe how data provided to a third-party contractor will be stored:

A. Data is stored using a cloud or infrastructure owned and hosted by a third party. Data is encrypted at rest in the database, and encrypted in transit with Secure Socket Layer enabled with AES-256.

B. Please describe the security protections that will be taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices:

Based on Discovery Education's security risk assessments and ongoing security monitoring, Discovery Education gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks, and new opportunities for managing security risks and incidents. Discovery Education uses this information to update and improve its risk assessment strategy and control processes.

Discovery Education has a comprehensive vulnerability management program that includes regular automated scans, and a suite of cybersecurity tools including endpoint protection and firewalls, with 24/7 monitoring provided by a Managed Security Services Provider (MSSP).

Part 6: Encryption Practices

☐ X By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).

By signing below, you agree that the information provided in the agreement is accurate and you agree to comply with the terms of the agreement and the Parents' Bill of Rights for Data and Security.

DocuSigned by:
Megan Haller
D661C3CCF863464...

Authorized VENDOR Signature — Date August 1, 2024

Authorized CUSTOMER Signature — Date 8/5/2024