



**PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY VENDOR SUPPLEMENT**

The Discovery Education, Inc. (the “Vendor”) has been engaged by the Trumansburg Central School District (the “District”) to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII).

The Vendor will use PII for the following exclusive purposes (*describe specific purpose for which the PII will be used*).

Discovery Education does not receive PII from the District. 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.

The Vendor will ensure that any subcontractors, assignees, or other agents that may access or receive PII will abide by the data protection and security requirements of District policy, and state and federal law and regulations by (*describe methods/procedures to safeguard data use by subcontractors*).

The Vendor will ensure that its personnel and subcontractors that may 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 Vendor will take all reasonable steps and to ensure the reliability of Vendor’s personnel and subcontractors that may access student data.

The Vendor uses the following third party contractor(s) to provide services to the District (*list third party contractors*):

Heroku
Mode Analytics, Inc.
Sendgrid (Part of Twilio)
Wistia, Inc.

PII will be stored (*describe the location in a manner that protects data security*).

Data is encrypted at rest in the database, and encrypted in transit with Secure Socket Layer enabled with AES-256.

Parents can challenge the accuracy of any student PII stored by Vendor by following the District's procedure for requesting the amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers and principals may be able to challenge accuracy of APPR data stored by Vendor by following the appeal procedure in the District's APPR Plan. Such challenges may be made by contacting Vendor at (*insert contact information, including title, phone number, mailing address and email address*):

Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 45 days of receiving the District’s written request. Contact information: education_info@discoveryed.com, 800-323-9084

The Vendor will take reasonable measures, to ensure the confidentiality of PII by implementing the following (*describe the measures used by to protect PII including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection*):

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).

The Vendor's agreement with the District begins on July 1, 2 and ends on June 30, .

Once the Vendor has completed its service to the District, records containing PII will be exported to the District. The Vendor shall thereafter securely delete and overwrite any and all PII remaining in the possession of the 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 PII maintained on behalf of the Vendor in secure data center facilities. The Vendor shall ensure that no copy, summary or extract of the PII or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities. Upon expiration of this Contract with a successor agreement in place, the Vendor will cooperate with the District as necessary to transition PII to the successor Vendor prior to deletion. The Vendor shall thereafter securely delete and overwrite any and all PII remaining in the possession of the 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 PII maintained on behalf of the Vendor in secure data center facilities. The Vendor shall ensure that no copy, summary or extract of the PII or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities

Vendor's Signature:  D661C3CCF063464...

Date: July 2, 2024

Printed Name and Title: Megan Haller, Global Head of Operations



DATA PRIVACY RIDER FOR ALL CONTRACTS INVOLVING PROTECTED DATA
PURSUANT TO EDUCATION LAW §2-C AND §2-D

Trumansburg Central School District (the “District”) and Discovery Education, Inc. (the “Vendor”) agree as follows:

1. Definitions:

(a) Personally Identifiable Information (PII) means the same as defined by New York Education Law §2-d.

2. Confidentiality of all PII shall be maintained in accordance with State and Federal Law and the District's Data Security and Privacy Policy.

3. The Parties agree that the District's Parents' Bill of Rights for Data Privacy and Security are incorporated as part of this agreement, and Vendor shall comply with its terms.

4. Vendor agrees to comply with Education Law §2-d and its implementing regulations.

5. Vendor agrees that any officers or employees of Vendor, and its assignees who have access to PII, have received or will receive training on federal and State law governing confidentiality of such data prior to receiving access to PII.

6. Vendor 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. Unauthorized use specifically includes, but is not limited to, selling or disclosing PII for marketing or commercial purposes, as those terms are defined under the implementing regulations, or permitting, facilitating, or disclosing such information to a third party for marketing or commercial purposes, as those terms are defined under the implementing regulations;

(c) except for authorized representatives of the third party contractor to the extent necessary to carry out the contract, 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 the statute or court order;

(d) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII 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 NIST Cybersecurity Framework;

(g) impose all the terms of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to PII; and

(h) work with the District to create the supplement to the Parents' Bill of Rights for Data Privacy and Security that meets the requirements of Education Law §2-d and its implementing regulations and which shall be incorporated as part of this agreement and posted on the District's website.

7. This Data Privacy Rider shall cover all services provided by Vendor to the District.

8. In the event of any conflict between the terms of this Data Privacy Rider and the agreement, the terms of this Data Privacy Rider shall control.

Vendor Discovery Education, Inc.

Signature  D661C3CCF063464...

Date: July 2, 2024

Name, Title Megan Haller, Global Head of Operations

Certificate Of Completion

Envelope Id: 96577517E5B049F081635EF7350DE94D	Status: Completed
Subject: Complete with DocuSign: DPA_NY_MS_TRUMANSBURG CENTRAL SCHOOL DISTRICT_2024	
Source Envelope:	
Document Pages: 4	Signatures: 2
Certificate Pages: 2	Initials: 2
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Melissa Bearor
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	4350 Congress St, Suite 700
	Charlotte, NC 28209
	MBearor@Discovered.com
	IP Address: 71.246.245.139


Record Tracking

Status: Original	Holder: Melissa Bearor	Location: DocuSign
7/2/2024 4:43:09 PM	MBearor@Discovered.com	

Signer Events

Kim Luong
 KLuong@discovered.com
 Paralegal
 Discovery Education
 Security Level: Email, Account Authentication (None)

Signature




Signature Adoption: Pre-selected Style
 Using IP Address: 71.127.54.65

Timestamp

Sent: 7/2/2024 4:45:37 PM
 Viewed: 7/2/2024 4:49:24 PM
 Signed: 7/2/2024 4:49:48 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Megan Haller
 MHaller@discovered.com
 Global Head of Operations
 Discovery Education
 Signing Group: Final Signer: DE Signatory
 Security Level: Email, Account Authentication (None)



Signature Adoption: Pre-selected Style
 Using IP Address: 174.219.7.6
 Signed using mobile

Sent: 7/2/2024 4:49:49 PM
 Viewed: 7/2/2024 4:55:22 PM
 Signed: 7/2/2024 4:55:31 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/2/2024 4:45:37 PM
Certified Delivered	Security Checked	7/2/2024 4:55:22 PM
Signing Complete	Security Checked	7/2/2024 4:55:31 PM

Envelope Summary Events	Status	Timestamps
Completed	Security Checked	7/2/2024 4:55:31 PM
Payment Events	Status	Timestamps