



EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Discovery Education, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Ulster County BOCES ("BOCES") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that Ulster County BOCES' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster County BOCES. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of Ulster County BOCES as that term is defined in § 99.3 of FERPA,

-AND-

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with Ulster County BOCES policy(ies) on data security and privacy. In the event this Agreement expires, is not renewed or is terminated, Contractor shall

destroy/delete all of Ulster County BOCES' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster County BOCES' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies how Protected Data will be deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Ulster County BOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, BOCES board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of Ulster County BOCES' Parent Bill of Rights.

NAME OF PROVIDER: Discovery Education, Inc.

BY:  **DATED:** November 10, 2020
78B6C33846AB459... _____

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

DISCOVERY EDUCATION STUDENT DATA PROTECTION ADDENDUM

This Discovery Education Student Data Protection Addendum (“**DPA**”) describes Discovery’s obligations to protect Student Data (defined below) during Discovery’s provision the Services to Subscriber.

1. Student Data and Purpose of DPA. As between Subscriber and Discovery, Subscriber or the party who provided such data (such as the student or parent), is the exclusive owner of all right, title, and interest in and to any and all Student Data disclosed or transmitted to Discovery under the Agreement and this DPA. Discovery hereby waives any and all statutory and common law liens it may now or hereafter have with respect to Subscriber’s Student Data. Nothing in the Agreement or this DPA will operate as an obstacle to Subscriber’s right to retrieve any and all Student Data disclosed or transmitted to Discovery under the Agreement and this DPA. Notwithstanding the foregoing, Discovery may de-identify and aggregate Subscriber’s Student Data with Discovery’s other Subscribers’ Student Data and use and exploit the de-identified and aggregate data for any lawful purpose. The parties agree to comply with the terms of this Addendum and Data Protection Laws as they relate to Student Data.

2. Schedule A (Discovery’s Security Policy). Schedule A attached hereto and incorporated herein sets forth Discovery’s policies regarding: (i) what steps Discovery takes to protect personally identifiable information (“**PII**”) that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII. For purposes of this DPA, PII includes Student Data.

3. Consents and Notifications for Disclosures of Student Data. Subscriber affirms, represents, and warrants that it has obtained, and is solely responsible for obtaining, all consents as may be required by the Data Protection Laws, as well as making all required disclosures to the parents, legal guardians, and students as may be required by the Data Protection Laws, to disclose or transmit Student Data to Discovery. Subscriber will provide proof of the required consent within 5 business days of Discovery’s written request.

4. Discovery’s Personnel and Subcontractors. Discovery 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. Discovery will take all reasonable steps and to ensure the reliability of Discovery personnel and subcontractors that access Student Data.

5. Student Data Requests. Discovery will, without undue delay, notify, then record, and then refer to Subscriber full details of all Student Data Requests. To the extent Subscriber is unable to respond to a Student Data Request with information available through Discovery’s products or services, Discovery will provide reasonable assistance to Subscriber in responding to a Student

Data Request. Discovery will not respond to a Student Data Request without Subscriber's explicit instruction.

6. Deletion or Return Of Student Data. Upon termination or expiration of the Agreement, Discovery will promptly, but without undue delay, destroy Student Data upon Subscriber's written request. Discovery may retain Student Data to the extent required by the laws, rules, and regulations to which Discovery is subject, or if Student Data resides in Discovery's backup archives, Discovery will continue to protect the security and confidentiality of such retained Student Data in accordance with the Agreement and this DPA. Discovery has implemented retention rules so that Student Data in backup archives is retained for as short a time as necessary.

7. Audits. Subscriber may request once per calendar year to audit Discovery's Security Policy and related systems that are used to store Student Data in order to verify compliance with this DPA and the Data Protection Laws. If Subscriber wishes to conduct an audit using a third party auditor, Discovery may object to Subscriber's choice of third party auditor on reasonable grounds and in such event, Subscriber will select a different auditor. Subscriber will reimburse Discovery for any time expended in relation to such audit at Discovery's then-current hourly professional services rate. Subscriber and Discovery will mutually agree upon the scope and timing of an audit prior to any such audit. An audit performed pursuant to this DPA will not exceed one business day and will not unreasonably interfere with the normal conduct of Discovery's business. Subscriber (or Subscriber's third-party auditor) will at all times comply with the use, security, and access policies at such location. Any audit performed pursuant to this Section DPA will be conducted under a confidentiality agreement and any information or report derived from such audit will be deemed Discovery's confidential information.

8. Student Data Breach.

8.1. Student Data Breach Notification. In the event of any Student Data Breach, upon Discovery becoming aware of such Student Data Breach, without undue delay Discovery will:

8.1.1. notify Subscriber of the Student Data Breach; and

8.1.2. provide Subscriber with details that are available to Discovery at the time of notice regarding:

- (a) the nature of the Student Data Breach, including the categories and approximate numbers of students and Student Data records concerned;
- (b) any investigations into such Student Data Breach; and
- (c) any measures taken to address the Student Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of the Student Data Breach.

8.2. Notification Sharing. Subscriber may share any notification and details provided by Discovery under this Section 11 with the appropriate government agency or law enforcement authority if required to do so under the Data Protection Laws.

9. Suspension. Subscriber may suspend the transfer of Student Data to Discovery, or terminate the affected Agreement without penalty to Subscriber if: (i) Discovery is in material breach of its obligations under this DPA and does not cure such breach within thirty (30) days of Subscriber's notification to Discovery of such breach; or (ii) Discovery notifies Subscriber that it cannot comply with the obligations set forth in this DPA or the Data Protection Laws.

10. Student Data Disclosures. To the extent legally permissible, Discovery will promptly notify Subscriber of any legally binding request for disclosure or seizure of Student Data by a government agency or law enforcement authority.

11. Term. The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement; or (ii) when all Student Data is deleted from Discovery's systems.

12. Indemnification. Each of the parties ("**Indemnifying Party**") agrees to indemnify and hold harmless the other party and its officers, employees, directors, and agents ("**Indemnified Party**") from, and at the Indemnifying Party's option defend against, any and all third party claims, losses, liabilities, damages, costs, and expenses (including attorneys' fees, consultants' fees, and court costs) (collectively, "**Claims**") arising out of the Indemnifying Party's (i) violation of a Data Protection Law; or (ii) breach of any provision of this DPA.

13. Definitions and Interpretation.

13.1. Definitions.

"**Data Protection Law**" means:

- (a) the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR part 99) ("**FERPA**");
- (b) the Children's Online Privacy and Protection Act (15 U.S.C. §§ 6501–6506) ("**COPPA**");
- (c) the Colorado Student Data Transparency and Security Act (C.R.S. 22-16-101 et.al.);
- (d) the Connecticut Public Act 16-189;
- (e) the California Consumer Privacy Act of 2018 ("**CCPA**");
- (f) the California Student Online Student Information Protection Act (**SB-1177**) ("**SOPIPA**");
- (g) the California Assembly Bill No. 1584;
- (h) the New York State Education Law § 2-d
- (i) the Canada Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and

- (j) all other federal and state data protection and breach notification laws applicable to Student Data;

in each case, as in force and applicable, and as may be amended, supplemented, or replaced from time to time.

“**Student Data**” means any personally identifiable information of a student that through the course of Subscriber’s use of the Services is: (i) provided by a student, or the student’s parent or legal guardian, to Discovery in the course of the student’s, parent’s, or legal guardian’s use of Discovery’s website, service, or application that is designed and marketed for K–12 school purposes; (ii) created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to Discovery; or (iii) gathered by Discovery through the operation of Discovery’s website, service, or application that is designed and marketed for K–12 school purposes and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact.

“**Student Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Student Data; and

“**Student Data Request**” means a request made by Subscriber, a parent or legal guardian, or student to exercise any rights granted by the Data Protection Laws.

Schedule 1

DISCOVERY EDUCATION, INC. DATA SECURITY POLICY

This Policy describes, in general, (i) what steps Discovery takes to protect personally identifiable information ("PII") that is provided to Discovery; (ii) how PII may be used; (iii) with whom Discovery may share PII, and (iv) the steps Discovery takes to protect the PII.

No student PII is required for the use of any of the basic Discovery Education services, however, in the event Users elect to use any of the functionality within the Discovery Education services which provide personalized pages, individual accounts, other user-specific customization, or otherwise submit or upload information (all such data is generally limited to the following: school name, first name, last name, grade level, and Discovery generated username/password), all such PII provided to Discovery will be protected in accordance with this Policy.

No school employee PII is required for Professional Development Services other than first name and last name for the purposes of attendance logs.

I. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

"Authorized Disclose" means the following: (1) third parties to whom the Subscriber/Customer/Distributor has given Discovery written approval to disclose PII; (2) third parties to whom disclosure is required by law; and (3) if applicable, third party vendors working on Discovery's behalf or performing duties in connection with Discovery's services (e.g. hosting companies) and who are required to implement administrative, physical, and technical infrastructure and procedural safeguards in accordance with accepted industry standards.

"Authorized Use" means a Discovery employee authorized by the Subscriber/Customer/Distributor to access PII in order to perform services under an Agreement.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S Department of Education and are available at <http://www2.ed.gov/policy/gen/reg/ferpa/index.html>.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA.

II. PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION

Basic Privacy Protections

1. Compliance with Law and Policy. All PII provided to Discovery is handled, processed, stored, transmitted and protected by Discovery in accordance with all applicable federal data privacy and security laws (including FERPA) and with this Policy.
2. Training. Employees (including temporary and contract employees) of Discovery are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security.
3. Personnel Guidelines. All Discovery employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. Discovery, and its respective personnel do not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or if there is legitimate need for the information to maintain data systems or to perform required services under the Agreement with Subscriber/Customer/Distributor. The following provides a general description of the internal policies to which Discovery and its respective personnel adhere:
 - a. Limit internal access to PII to Discovery personnel with proper authorization and allow use and/or disclosure internally, when necessary, solely to personnel with a legitimate need for the PII to carry out the services provided under the Agreement.
 - b. Disclose PII only to Authorized Disclosees
 - c. Access PII only by Authorized Users.
 - d. When PII is no longer needed, delete access to PII.
 - e. Permit employees to store or download information onto a local or encrypted portable devices or storage only when necessary, and to create a written record for retention verifying that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).
 - f. Any downloaded materials consisting of PII remain in the United States.
 - g. Prohibit the unencrypted transmission of information, or any other source of PII, wirelessly or across a public network to any third party.
 - h. Upon expiration or termination of Agreement, Discovery shall Destroy all PII previously received from Subscriber/Customer/Distributor no later than sixty (60) days following such termination, unless a reasonable written request is submitted by Subscriber/Customer/Distributor to Discovery to hold such PII. Each electronic file containing PII provided by Subscriber/Customer/Distributor to Discovery will be securely Destroyed. This provision shall apply to PII that is in the possession of Discovery, Discovery employees/personnel and/or Authorized Disclosees.

Information Security Risk Assessment

Discovery periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Discovery; Discovery reports such risks as promptly as possible to

Subscribers/Customers/Distributors; and Discovery implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented by Discovery based on the level of risks, capabilities, and operating requirements. These measures include, as appropriate and reasonable, the following safeguards:

1. Administrative Safeguards

- a. Sanctions: Appropriate sanctions against Contractor personnel who fail to comply with Discovery's security policies and procedures.
- b. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
- c. Security Oversight: Assignment of one or more appropriate management level employees of Discovery to be responsible for developing, implementing, and monitoring of safeguards and security issues.
- d. Appropriate Access: Procedures to determine that the access of Discovery personnel to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Discovery personnel who have access to PII.
- e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to PII.
- f. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

2. Physical Safeguards

- a. Access to PII: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
- b. Awareness Training: On-going security awareness through training or other means that provide Discovery personnel (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training also addresses procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.
- c. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
- d. Physical Access: Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.
- e. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.

f. **Operational Environment:** Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where PII is stored.

g. **Media Movement:** Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.

3. Technical Safeguards

a. **Data Transmissions:** Technical safeguards, including encryption, to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups.

b. **Data Integrity:** Procedures that protect PII maintained by Discovery from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.

c. **Logging off Inactive Users:** Inactive electronic sessions are designed to terminate automatically after a specified period of time.

Security Controls Implementation

Discovery has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

Security Monitoring

In combination with periodic security risk assessments, Discovery uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Discovery also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.

Security Process Improvement

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

Audit

Discovery acknowledges Subscriber's/Customer's/Distributor's right to audit any PII collected by Discovery and/or the security processes listed herein upon reasonable prior written notice to Discovery's principal place of business, during normal business hours, and no more than once per year. Discovery shall maintain records and documentation directly and specifically related to the services performed under the Agreement for a period of three (3) years, unless otherwise stated in Section II(3)(h) of this Policy.

Breach Remediation

Discovery keeps PII provided to Discovery secure and uses reasonable administrative, technical, and physical safeguards to do so. Discovery maintains and updates incident response plans that establish procedures in the event a breach occurs. Discovery also identifies individuals responsible for implementing incident response plans should a breach occur.

If a Subscriber/Customer/Distributor or Discovery determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Discovery provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws.

Discovery reports as promptly as possible to Subscribers/Customers/Distributors (or their designees) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. Such incidents include any breach or hacking of Discovery's Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Discovery's business, whether or not owned by Discovery or operated by its employees or agents in performing work for Discovery.

Personnel Security Policy Overview

Discovery mitigates risks by:

1. Performing appropriate background checks and screening of new personnel, in particular those who have access to PII.
2. Obtaining agreements from internal users covering confidentiality, nondisclosure and authorized use of PII.
3. Providing training to support awareness and policy compliance for new hires and annually for personnel.



PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law §2-d, Ulster BOCES wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any marketing or 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 the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 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:

Ulster BOCES
175 Route 32 North
New Paltz, New York 12561

or

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234

Complaints may also be directed to the
Chief Privacy Officer (CPO) via e-mail at
CPO@mail.nysed.gov

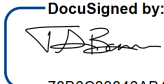
6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data as well as teacher or principal data.

Supplemental Information Regarding Third Party Contractors

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to “student data” and/or “teacher or principal data,” as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used by third party contractor;
2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
4. If and 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;
5. Where the student data or teacher or principal 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 and data security and privacy risks mitigated.
6. Address how the data will be protected using encryption while in motion and at rest.

DocuSigned by:

Signature: _____
78B6C33846AB459...

Print Name: Travis Barrs

Title: COO

Company Name: Discovery Education, Inc.

Date: November 10, 2020

Certificate Of Completion

Envelope Id: 9560CA8C273E4824A5278BA5A2356655	Status: Completed
Subject: Please DocuSign: PRESIGN_NY_Ulster BOCES_RIDER.pdf, PRESIGN_NY_Ulster BOCES_DATA PRIVACY.pdf	
Source Envelope:	
Document Pages: 14	Signatures: 2
Certificate Pages: 2	Initials: 2
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Melissa Bearor
Time Zone: (UTC-05:00) Eastern Time (US & Canada)	MBearor@Discovered.com
	IP Address: 71.163.75.173

Record Tracking

Status: Original	Holder: Melissa Bearor	Location: DocuSign
11/10/2020 12:51:03 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: 71.114.26.223

Timestamp

Sent: 11/10/2020 12:53:09 PM
 Viewed: 11/10/2020 12:53:42 PM
 Signed: 11/10/2020 12:54:20 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Travis Barrs
 tbarrs@discovered.com
 COO
 Discovery Education
 Signing Group: Final Signer: DE Signatory
 Security Level: Email, Account Authentication (None)

DocuSigned by:

 78B6C33846AB459...

Signature Adoption: Drawn on Device
 Using IP Address: 107.127.31.175
 Signed using mobile

Sent: 11/10/2020 12:54:23 PM
 Viewed: 11/10/2020 6:31:22 PM
 Signed: 11/10/2020 6:31:33 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	11/10/2020 12:53:09 PM
Certified Delivered	Security Checked	11/10/2020 6:31:22 PM
Signing Complete	Security Checked	11/10/2020 6:31:33 PM
Completed	Security Checked	11/10/2020 6:31:33 PM

Payment Events

Status

Timestamps