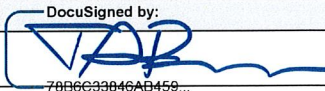


## APPENDIX A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the BOCES directly (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

<b>CONTRACTOR</b>	
<b>Signature:</b>	
<b>Printed Name:</b>	<b>Travis Barrs</b>
<b>Title:</b>	<b>Head of Global Operations</b>
<b>Date:</b>	April 28, 2022


## APPENDIX B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -  
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE  
INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	<b>Discovery Education, Inc.</b>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	<b>To provide digital educational services such as Discovery Education Experience, Coding, Science, STEM Connect, and Professional Learning.</b>
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII for Discovery Education; but Mystery Science does not collect Student Data. <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>July 1, 2022</u> Contract End Date <u>June 30, 2025</u>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract and upon request of BOCES, Contractor shall securely delete and destroy Student Data.
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting BOCES. If a correction to data is deemed necessary, BOCES will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving BOCES's written request.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:

	<p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: <b>The Contractor will store the EA's data in several hosting sites in the U.S. The Contractor 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). Data from BOCES is uploaded via a secure FTP site. Only internal employees with appropriate access level approved by management will have access to BOCES data. Data is encrypted at rest in the database. We perform daily onsite backup as well as offsite backup.</b></p>
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

CONTRACTOR	
<b>Signature:</b>	 <small>78B6C33846AB459...</small>
<b>Printed Name:</b>	<b>Travis Barrs</b>
<b>Title:</b>	<b>Head of Global Operations</b>
<b>Date:</b>	April 28, 2022



## APPENDIX C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to BOCES's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	The comprehensive Contractor's Data Privacy Addendum can be found here: <a href="https://www.discoveryeducation.com/data-%20protection-addendum/">https://www.discoveryeducation.com/data-%20protection-addendum/</a> and the Privacy Policy can be found here: <a href="https://www.discoveryeducation.com/privacy-policy/">https://www.discoveryeducation.com/privacy-policy/</a> .
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>1. <u>Administrative Safeguards</u> 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 Personal Information 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 Personal Information. e. Employee Supervision: Procedures for regularly monitoring and supervising Discovery personnel who have access to Personal Information. f. Access Termination: Procedures for terminating access to Personal Information when employment ends, or when an individual no longer has a legitimate need for access.</p> <p>2. <u>Operational Safeguards</u> a. Access to Personal Information: Procedures that grant access to Personal Information 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</p>

		<p>physical access to Personal Information 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 Personal Information. 6 Student DPA with Security Policy updated 6/30/2021 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 Personal Information is stored. g. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain Personal Information into and out of a facility.</p> <p>3. <u>Technical Safeguards</u> a. Data Transmissions: Technical safeguards, including encryption, to ensure Personal Information transmitted over an electronic communications network is not accessed by unauthorized persons or groups. b. Data Integrity: Procedures that protect Personal Information 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.</p>
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	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 that personnel receive annual training regarding the appropriate federal and state laws. Discovery will also ensure that personnel are bound by appropriate obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	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 contractual 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 Vendor's personnel and subcontractors that access student data.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or	Contractor maintains and updates incident response plans that establish procedures in the event a breach occurs. Contractor also identifies individuals responsible for implementing incident response plans should a breach occur. In combination with periodic security risk assessments, Discovery Education uses a variety of approaches and technologies to make sure that risks and



	<p>unauthorized disclosures, and to meet your obligations to report incidents to BOCES.</p>	<p>incidents are appropriately detected, assessed and mitigated on an ongoing basis. Discovery Education also assesses on an ongoing basis whether controls are effective and perform as intended, including intrusion monitoring and data loss prevention.</p> <p>If BOCES/customer/distributor or Contractor determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Contractor 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.</p> <p>Contractor reports as promptly as possible to BOCES/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 personally identifiable information of which they become aware. Such incidents include any breach or hacking of Contractor'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 Contractor's business, whether or not owned by Contractor or operated by its employees or agents in performing work for the Contractor.</p>									
6	Describe how data will be transitioned to BOCES when no longer needed by you to meet your contractual obligations, if applicable.	Upon BOCES request, Contractor shall Destroy all Student Data previously received from BOCES no later than sixty (60) days following such request.									
7	Describe your secure destruction practices and how certification will be provided to BOCES.	Upon BOCES request, Contractor shall Destroy all Student Data previously received from BOCES no later than sixty (60) days following such request.									
8	Outline how your data security and privacy program/practices align with BOCES's applicable policies.	The comprehensive Contractor's Data Privacy Addendum can be found here: <a href="https://www.discoveryeducation.com/data-%20protection-addendum/">https://www.discoveryeducation.com/data-%20protection-addendum/</a> and the Privacy Policy can be found here: <a href="https://www.discoveryeducation.com/privacy-policy/">https://www.discoveryeducation.com/privacy-policy/</a> .									
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	<p>Cybersecurity Frameworks</p> <table border="1"> <thead> <tr> <th></th><th>MAINTAINING ORGANIZATION/GROUP</th><th>FRAMEWORK(S)</th></tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td><td>National Institute of Standards and Technology</td><td>NIST Cybersecurity Framework Version 1.1</td></tr> <tr> <td><input checked="" type="checkbox"/></td><td>National Institute of Standards and Technology</td><td>NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171</td></tr> </tbody> </table>		MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)	<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1	<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)									
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1									
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171									

## APPENDIX C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	NCSR 5 implementation in progress
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	NCSR 4 – some activities are still being documented
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	NCSR 5 implementation in progress
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	NCSR 5 implementation in progress
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	NCSR 5 implementation in progress
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	NCSR 5 implementation in progress
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to	NCSR 5 implementation in progress



Function	Category	Contractor Response
	physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	NSCR 5 implementation in progress
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	NSCR 6 Tested and Verified
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	NSCR 5 implementation in progress
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	NSCR 6 Tested and Verified
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	NSCR 6 Tested and Verified
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	NSCR 6 Tested and Verified
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	NSCR 6 Tested and Verified
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NSCR 6 Tested and Verified
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	NSCR 6 Tested and Verified
	<b>Communications (RS.CO):</b> Response	NSCR 5 implementation in progress



Function	Category	Contractor Response
	activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	NSCR 6 Tested and Verified
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	NSCR 6 Tested and Verified
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	NSCR 5 implementation in progress - currently implementing process improvements
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	NCSR 5 Implementation in progress. Process is documented but not tested and verified
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	NSCR 5 implementation in progress - currently implementing process improvements
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	NSCR 5 implementation in progress - this is difficult to test holistically, however we are confident in our planning.