EXHIBIT B

NEW YORK DATA PRIVACY AGREEMENT

OCM BOCES

and

DISCOVERY EDUCATION, INC.

This Data Privacy Agreement ("DPA") is by and between the BOCES listed in the space provided above, ("BOCES"), an Educational Agency, and Discovery Education, Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school , board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family

Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

- **Compliance with Law.**

In order for Contractor to provide certain services ("Services") (as listed in Appendix A) to BOCES pursuant to the BOCES Purchase Contract ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("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); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

- **Authorized Use.**

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

- **Data Security and Privacy Plan**.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and BOCES's policies. Education Law Section 2-d requires that Contractor provide BOCES with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements.

- **BOCES's Data Security and Privacy Policy**
  State law and regulation requires BOCES to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with BOCES's data security and privacy policy and other applicable policies.

- **Right of Review and Audit.**
  Upon request by BOCES, Contractor shall provide BOCES with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required, no more than once per calendar year and during normal working hours, to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, BOCES's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to BOCES. Contractor may provide BOCES with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

- **Contractor's Employees and Subcontractors**.
  (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors have entered into written agreements with Contractor.
  (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to Student Data will abide by the Contractor's Student Data Protection Addendum, found at https://www.discoveryeducation.com/data-%20protection-addendum/ that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
  (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point, to the Contractor's knowledge, a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify BOCES and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
  (d) Contractor shall take full responsibility for the negligent acts and omissions of its employees and subcontractors as it relates to this Data Privacy Agreement and the underlying Agreement in Appendix D.
  (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify BOCES of the court order or subpoena in advance of

compliance but in any case, provides notice to BOCES no later than the time the PII is disclosed, unless such disclosure to BOCES is expressly prohibited by the statute, court order or subpoena.

- **Training**.
  Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

- **Termination**
  The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII or it is replaced by another data agreement.

- **Destruction of Data**.
  (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to BOCES, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to BOCES, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by BOCES for purposes of facilitating the transfer of PII to BOCES or expressly required by law.

  (b) If applicable, upon expiration or termination of the Service Contractor or upon request by the BOCES, Contractor agrees to destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

  (c) Upon request, Contractor shall provide BOCES with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

  (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

- **Commercial or Marketing Use Prohibition.**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

- **Encryption.**
  Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

- **Breach**.
  (a) Contractor shall promptly notify BOCES of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist BOCES. Notifications required by this section must be sent to BOCES's Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify BOCES shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

  (b) Notifications required under this paragraph must be provided to BOCES at the following address:

Name: Phillip D Grome

Title: Assistant Superintendent for Admin

OCM BOCES BOCES

Address: PO BOX 4754

Syracuse, NY 13221

Email: pgrome@ocmboces.org

Cooperation with Investigations.

Contractor agrees that it will cooperate with BOCES and law enforcement, where necessary, in any investigations into a Breach. Any reasonable costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

- **Notification to Individuals.**
  Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or

promptly reimburse BOCES for the full reasonable cost of BOCES's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

- **Termination**.
  The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
   Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by BOCES. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within sixty (60) calendar days to BOCES's requests for access to Student Data so BOCES can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify BOCES and refer the Parent or Eligible Student to BOCES.

2. **Bill of Rights for Data Privacy and Security**.
   As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Appendix A and Appendix B, respectively, and incorporated into this DPA. Contractor shall complete and sign Appendix B and append it to this DPA. Pursuant to Education Law Section 2-d, BOCES is required to post the completed Appendix B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**
   In the event of a conflict between and among the terms and conditions of this DPA, including all Appendixes attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**
   This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
By: Phil Grome	By:
Name: Phil Grome	Travis Barrs
Title: Assistant Superintendent for Administration	Head of Global Operations
Date: 9/4/22	Date:

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 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, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to 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.

CONTRACTOR	
Signature:	
Printed Name:	**Travis Barrs**
Title:	**Head of Global Operations**
Date:	

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).

Name of Contractor	**Discovery Education, Inc.**
Description of the purpose(s) for which Contractor will receive/access PII	**To provide digital educational services such as Discovery Education Experience, Coding, Science, STEM Connect, and Professional Learning.**
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII for Discovery Education; but Mystery Science does not collect Student Data. ☐ APPR Data
Contract Term	Contract Start Date 7/1/2022 Contract End Date 6/30/2023
Subcontractor Written Agreement Requirement	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) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract and upon request of BOCES, Contractor shall securely delete and destroy Student Data.
Challenges to Data Accuracy	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.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other:

	Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: **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.**
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	
Printed Name:	**Travis Barrs**
Title:	**Head of Global Operations**
Date:	

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 esure 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: https://www.discoveryeducation.com/data-%20protection-addendum/ and the Privacy Policy can be found here: https://www.discoveryeducation.com/privacy-policy/.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	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 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. 2. Operational Safeguards 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

		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. 3. Technical Safeguards 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.
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

	unauthorized disclosures, and to meet your obligations to report incidents to BOCES.	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. 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. 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.
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: https://www.discoveryeducation.com/data-%20protection-addendum/ and the Privacy Policy can be found here: https://www.discoveryeducation.com/privacy-policy/.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	Cybersecurity Frameworks ☑ National Institute of Standards and Technology — NIST Cybersecurity Framework Version 1.1 ☑ 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)	**Asset Management (ID.AM):** 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.	NSCR 5 implementation in progress
	Business Environment (ID.BE): 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.	NSCR 4 – some activities are still being documented
	Governance (ID.GV): 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.	NSCR 5 implementation in progress
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	NSCR 5 implementation in progress
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	NSCR 5 implementation in progress
	Supply Chain Risk Management (ID.SC): 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.	NSCR 5 implementation in progress
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to	NSCR 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.	
	Awareness and Training (PR.AT): 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
	Data Security (PR.DS): 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
	Information Protection Processes and Procedures (PR.IP): 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
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	NSCR 6 Tested and Verified
	Protective Technology (PR.PT): 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)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	NSCR 6 Tested and Verified
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	NSCR 6 Tested and Verified
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	NSCR 6 Tested and Verified
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	NSCR 6 Tested and Verified
	Communications (RS.CO): 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).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	NSCR 6 Tested and Verified
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	NSCR 6 Tested and Verified
	Improvements (RS.IM): 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)	**Recovery Planning (RC.RP):** 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
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	NSCR 5 implementation in progress - currently implementing process improvements
	Communications (RC.CO): 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.