Appendix R
NEW YORK STATE EDUCATION DEPARTMENT'S
DATA PRIVACY APPENDIX

ARTICLE I: DEFINITIONS

As used in this Data Privacy Appendix ("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 New York 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 district, 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 § 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 district 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. **Services:** Services provided by Contractor pursuant to this contract with the NYS Education Department to which this Data Privacy Appendix is attached and incorporated.
14. **Student:** Any person attending or seeking to enroll in an Educational Agency.
15. **Student Data or Student Personally Identifiable Information:** Personally Identifiable Information as defined in § 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C § 1232g.
16. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of Services.
17. **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

1. **Compliance with Law.**

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 § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121. The Parties enter into 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. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

2. **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.

3. **Contractor's Data Privacy and Security 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, rules and regulations, and the NYS Education Department's ("NYSED") policies. Education Law § 2-d requires that Contractor provide NYSED 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 privacy and security requirements. Contractor's Data Privacy and Security Plan is attached to this DPA as DPA Exhibit 1.

4. **NYSED's Data Privacy and Security Policy**
State law and regulation require NYSED to adopt a data privacy and security 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 NYSED's Data Privacy and Security Policy located at http://www.nysed.gov/data-privacy-security/nysed-data-privacy-and-security-policy and other applicable policies.

5. **Right of Review and Audit.**
Upon NYSED's request, Contractor shall provide NYSED with copies of its policies and related procedures that pertain to the protection of PII in a form that does not violate Contractor's confidentiality obligations and applicable laws. In addition, Contractor may be required 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, NYSED'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 NYSED. In lieu of performing an audit, Contractor may provide NYSED with an industry standard independent audit report on Contractor's privacy and security practices that is no more than twelve months old.

6. **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 comply with the terms of this DPA.

(b) Contractor must ensure that each Subcontractor performing Services where the Subcontractor will receive or have access to PII is contractually bound by a written agreement 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 privacy and security measures of its Subcontractors prior to utilizing the Subcontractor. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify NYSED 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 acts and omissions of its employees and Subcontractors.

(e) Other than Contractor's employees and Subcontractors, 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 NYSED of the court order or subpoena in advance of compliance but in any case, provides notice to NYSED no later than the time the PII is disclosed, unless such disclosure to NYSED is expressly prohibited by the statute, court order or subpoena.

7. **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.

8. **Data Return and Destruction of Data**.

(a) Contractor 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 term of the Contract unless such retention is either expressly authorized for a prescribed period by the Contract, expressly requested in writing by NYSED for purposes of

facilitating the transfer of PII to NYSED, or expressly required by law. As applicable, upon expiration or termination of the Contract, Contractor shall transfer PII, in a format agreed to by the Parties to NYSED.

(b) When the purpose that necessitated the receipt of PII by Contractor has been completed or Contractor's authority to have access to PII has expired, Contractor shall ensure that 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 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) Contractor shall provide NYSED with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors to the contact and address for notifications set forth in the Contract.

(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.

9. Commercial or Marketing Use Prohibition.

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

10. 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.

11. Breach.

Contractor shall promptly notify NYSED of any Breach of PII in the most expedient way possible and 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 mail, 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 name of a point of contact. Notifications required by this section must be sent to NYSED at the contact provided for contract related notifications with a copy to the Chief Privacy Officer, NYS Education Department, 89 Washington Avenue, Albany, New York 12234. Violations of the requirement to notify NYSED shall be subject to a civil penalty pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law § 2-d may subject the Contractor to additional penalties.

12. **Cooperation with Investigations.**
Contractor agrees that it will cooperate with NYSED, and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

13. **Notification to Individuals.**
Where a Breach of PII occurs that is attributable to Contractor and/or its Subcontractors, Contractor shall pay for or promptly reimburse NYSED the full cost of NYSED's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law § 2-d and 8 NYCRR Part 121.

14. **Termination**.
The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of the Agreement to which this DPA is attached as long as the Contractor or any of its Subcontractors retain PII or access to PII but shall terminate upon Contractor's certifying that it and all of its' Subcontractors have destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
Education Law § 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 NYSED. To the extent Student Data is held by Contractor pursuant to the Contract, Contractor shall respond within thirty (30) calendar days to NYSED's requests for access to Student Data

necessary for NYSED to 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 Contract, Contractor shall refer the Parent or Eligible Student to NYSED and notify NYSED.

2. **Bill of Rights for Data Privacy and Security**.
   As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the Supplemental Information for the Contract is included as DPA Exhibit 2 and incorporated into this DPA. Contractor shall complete and sign DPA Exhibit 2 and it shall be appended to this DPA. Pursuant to Education Law § 2-d, NYSED is required to post the Parents Bill of Rights for Data Privacy and Security and the Supplemental Information about each contract where the contractor will receive PII on its website.

DPA EXHIBIT 1 - Contractor's Data Privacy and Security Plan

The NYS Education Department (NYSED) is required to ensure that all contracts with a third-party contractor that receives PII include a Data Privacy and Security Plan, pursuant to Education Law § 2-d and § 121.6 of the Regulations of the Commissioner of Education. 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 NYSED'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 privacy and security contract requirements over the life of the Contract.	
2.	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	

5.	Specify how you will manage any data privacy and security incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the NYSED.	
6.	Describe how data will be transitioned to NYSED when no longer needed by you to meet your contractual obligations, if applicable.	
7.	Describe your secure destruction practices and how certification will be provided to the NYSED.	
8.	Outline how your data privacy and security program/practices align with NYSED's applicable policies.	
9.	Outline how your data privacy and security program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	**PLEASE USE TEMPLATE BELOW.**

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.	
	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.	
	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.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	

Function	Category	Contractor Response
	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.	
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to 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.	
	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.	
	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.	

Function	Category	Contractor Response
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	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.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	

Function	Category	Contractor Response
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
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.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	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).	

DPA EXHIBIT 2 - Education Law § 2-d Bill of Rights for Data Privacy and Security and Supplemental Information for Contracts that Utilize Personally Identifiable Information

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 (Student PII) cannot be sold or released for any Commercial or Marketing purpose. Student 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 Regulations of the Commissioner of Education 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 Student PII.

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 New York State Education Department ("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 Student PII addressed. (i) Complaints should 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 Student PII occurs.

8. NYSED workers that handle Student PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. NYSED contracts with vendors that receive Student PII will address statutory and regulatory data privacy and security requirements.

Supplemental Information

Pursuant to Education Law § 2-d and § 121.3 of the Regulations of the Commissioner of Education, the NYS Education Department ("NYSED") is required to post information to its website about its contracts with third-party contractors that will receive Student PII and/or Teacher and/or Principal APPR data ("APPR Data"), collectively referred to as PII.

Name of Contractor	
Description of the purpose(s) for which Contractor will receive/access PII	
Type of PII that Contractor will receive/access (Write Yes or N/A on the lines next to each item)	_____ Student PII _____ APPR Data
Contract Term	Contract Start Date: _____ Contract End Date: _____
Subcontractor Written Agreement Requirement (Write Yes or N/A on the lines next to each item)	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, Contractor shall: • Securely transfer data to NYSED, or a successor contractor at NYSED's option and written discretion, in a format agreed to by the parties**.** • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting NYSED. If a correction to data is deemed necessary, NYSED will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving NYSED's written request.
Secure Storage and Data Security (Write Yes or N/A on the lines next to each item)	Please describe where PII will be stored and the protections taken to ensure PII will be protected: _____ Using a cloud or infrastructure owned and hosted by a third party. _____ Using Contractor owned and hosted solution _____ Other: Please describe how data privacy and security risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

Contractor's Name	
Signature	
Printed Name	
Title	
Date	