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 Personal Information in a manner not permitted by New York State and federal laws, rules and regulations, or in a manner that 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 Personal Information.
2. **Disclose**: To permit access to, or the release, transfer, or other communication of Personal Information by any means, including oral, written or electronic, whether intended or unintended.
3. **Encrypt or Encryption**: The use of an algorithmic process to transform Personal 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.
4. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
5. **Personal Information:** Information concerning a natural person which, because of name, number, personal mark, or another identifier, can be used to identify such natural person.
6. **Release:** Shall have the same meaning as Disclose.
7. **Services:** Services provided by Contractor pursuant to the contract with the NYS Education Department to which this Data Privacy Appendix is attached and incorporated.
8. **Subcontractor:** Contractor's non-employee agents, consultants and/or any person or any person or entity engaged in the provision of Services pursuant to an agreement with or at the direction of the Contractor.

ARTICLE II: PRIVACY AND SECURITY OF PERSONAL INFORMATION

1. **Compliance with Law.**

   Contractor may receive Personal Information regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act at 12 U.S.C. § 1232g (34 CFR

Part 99); Children's Online Privacy Protection Act at 15 U.S.C. §§ 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment at 20 U.S.C. § 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); the New York Education Law at § 2-d (8 NYCRR Part 121); the New York General Business Law at article 39-F, and the New York Personal Privacy Protection Law at Public Officers Law article 6-A. Contractor agrees to maintain the confidentiality and security of Personal Information in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no rights or claims of ownership to Personal Information, and Contractor must not use Personal Information 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 Personal Information in a manner that complies with New York State, federal and local laws, rules and regulations. Contractor shall 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. **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 Personal Information 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 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.

5. **Contractor's Employees and Subcontractors**.
   (a) Contractor shall only disclose Personal Information to Contractor's employees and Subcontractors who need to know the Personal Information in order to provide the Services and the disclosure of Personal Information 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 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 Personal Information; and, as applicable, retrieve all Personal Information received or stored by such Subcontractor and/or ensure that Personal Information has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises Personal Information, 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 Personal Information 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 Personal Information is disclosed, unless such disclosure to NYSED is expressly prohibited by the statute, court order or subpoena.

6. Training.

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

7. Data Return and Destruction of Data.

(a) Contractor is prohibited from retaining Personal Information or continued access to Personal Information or any copy, summary or extract of Personal Information, on any storage medium (including, without limitation, secure data centers and/or cloud-based facilities, and hard copies) whatsoever beyond the term of the Contract unless such retention is either expressly authorized by the Contract, expressly requested in writing by NYSED for purposes of facilitating the transfer of Personal Information to NYSED, or expressly required by law. As applicable, upon expiration or termination of the Contract, Contractor shall transfer Personal Information, in a format agreed to by the Parties to NYSED.

(b) When the purpose that necessitated the receipt of Personal Information by Contractor has been completed or Contractor's authority to have access to Personal Information has expired, Contractor shall ensure that all Personal Information (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all Personal Information 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 Personal Information cannot be read, or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the Personal Information cannot be retrieved. Only the destruction of paper Personal Information, 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 Personal Information held by the Contractor or Subcontractors to the Agreement at the address for notifications set forth in the Agreement.

(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), Contractor agrees that neither it nor its Subcontractors will attempt to re-identify de-identified data and/or transfer de-identified data to any person or entity, except as provided in subsection (a) of this section.

8. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Personal Information.

9. Breach.

Contractor shall promptly notify NYSED of any Breach of Personal Information 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 Personal Information 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.

10. **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.

11. **Notification to Individuals.**
    Where a Breach of Personal Information 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 the affected individuals.

12. **Termination**.
    The confidentiality and data security obligations of Contractor under this DPA shall continue for as long as Contractor or its Subcontractors retain Personal Information or access to Personal Information and shall survive any termination of the Agreement to which this DPA is attached.

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

NYSED has adopted the NIST Cybersecurity Framework as its' standard to protect Personal Information. 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.	