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 (EA) 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	Frontline Technologies Group LLC d/b/a Frontline Education
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.
Description of the purpose(s) for which Contractor will receive/access PII	* Frontline Education collects personally identifiable information (PII) on individuals including administrators, educators, students, and other as outlined in the Frontline Technologies Group LLC Privacy Policy which is available at https://www.frontlineeducation.com/about/commitment-to-security/. * Frontline Education will only use PII as specifically permitted in agreements entered with customers. Specifically, PII is used for the provision of services and tracking of information across Frontline products and platforms. * Frontline Education may use de-identified, anonymized and aggregated data for various purposes including enhancing the customer experience and refining and developing additional products and services.

Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII
Contract Term	Contract Start Date 7/1/2026 Contract End Date 6/30/2027
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, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format as the data is maintained by Frontline. • Securely delete and destroy data. Backup files made in the normal course of business may be retained by Contractor's data retention policy, for regulatory compliance.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA'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: Frontline hosts its solutions within Amazon AWS and SunGard Availability Services Data Center(s) in a secured hybrid hosting model and maintains complete administrative control of customer data within these hosting environments. Frontline Education encrypts data within our production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using Full Disk Encryption and all database backups are AES-256 encrypted.Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: • Frontline encrypts data within its production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using Full Disk Encryption and all database backups are AES-256 encrypted. • Frontline secures all sensitive data in transit using strong encryption protocols to encrypt all traffic including use of TLS 1.2 protocols, and SHA2 signatures. • Frontline adheres to the principles of least privilege and role-based permissions

	when provisioning access ensuring workers are only authorized to access data as a requirement of their job function. All production access is reviewed annually, at a minimum.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) 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 the EA'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.	• Frontline collects personally identifiable information (PII) on individuals including administrators, educators, students and others as outlined in the Frontline Technologies Group LLC Privacy Policy which is available at https://www.frontlineeducation.com/about/commitment-to-security/. • Frontline will only use PII as specifically permitted in agreements entered with customers. PII is used for the provision of services and tracking of information across Frontline products and platforms. • Frontline may use de-identified, anonymized and aggregated data for various purposes including enhancing the customer experience and refining and developing additional products and services.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	• Frontline encrypts data within its production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using full disk encryption and all database backups are AES-256 encrypted. • Frontline secures all sensitive data in transit using strong encryption protocols to encrypt all traffic including use of TLS 1.2 protocols, and SHA2 signatures. • Frontline adheres to the principles of least privilege and role-based permissions when provisioning access ensuring workers are only authorized to access data as a requirement of their job function. All production access is reviewed annually, at a minimum.
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.	Training shall be provided, and agreed to, at least annually via an online learning management system.
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.	Frontline requires that all service providers complete a risk assessment. After the completion of a successful risk assessment, Frontline qualifies third-party contractors' products/services for use based on their need to interact with customer data. Frontline requires a SOC2 (or comparable) independent audit of third-party contractors' operations at least annually.
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 unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Investigate and provide Educational Agency with a detailed notice of the breach, including the date and time of breach, name(s) of the individual(s) whose data was released or disclosed, nature and extent of the breach, and measures taken to prevent such a future breach.

6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	After contract completion, a backup file of all student data will be generated. Data in the database will be in normalized tables. All binary data will be extracted and provided in a .ZIP file. This data is made available for the district to download via SFTP. 90 days after completion of the services contract, the data will be purged. Customer data will purge from backup systems as they cycle-out in accordance with our data retention policies.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Frontline disposes of all student data in accordance with NIST Special Publication 800-88 including hard drive Secure Erase commands to destruct electronic data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Frontline will not knowingly retain PII beyond the time required to support authorized educational/school purposes. Following termination or deactivation of a EA account, Frontline may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes. All student data associated with the EA will be deleted promptly. Frontline may maintain anonymized or aggregated data, including usage data, for analytics purposes to improve products and services.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please refer to our SOC2 report.

Western Suffolk BOCES 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.

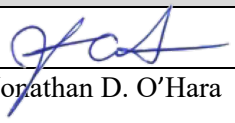
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org . (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]	Jonathan D. O'Hara
[Title]	VP, Controller
Date:	9/1/2026