

Appendix A
Compliance With New York State Education Law Section 2-d Addendum ("Addendum")

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Frontline, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings: "Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing; not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(c) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(d) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.);

(e) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(f) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(g) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(h) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(i) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts

located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(j) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(k) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(l) ensure that employees, assignees and agents of Contractor who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(m) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(<https://www.monroe.edu/domain/1478>)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (<https://www.monroe.edu/6320>)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or

Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between Frontline Technologies Group LLC (“Frontline”) and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide Frontline’s Professional Growth, Frontline Central, Recruiting and Hiring, and Special Ed & Interventions solutions to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be July 1, 2023 – June 30, 2024 and the Agreement shall remain in effect until [DATE], unless sooner by either party for any reason upon thirty (30) days’ notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be

retained in compliance with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.



June 2, 2023

Vendor Signature

ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none"> • 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 period required to support authorized educational/school purposes. Following termination or deactivation of a District 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 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(A) – 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.	Please see SOC 2 Type II Report for this table.
	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	
Function	Category	Contractor Response
	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.	
	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

	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	
	<p>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.</p>	
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous</p>	

	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	
Function	Category	Contractor Response
	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).	

Frontline Education Data Security and Privacy Plan Executive Summary

Frontline Technologies Group LLC, doing business as Frontline Education, has established a unified control framework based on the NIST Cyber Security Framework (CSF). Frontline has several security control standards that are applicable to its product development and operations environments. Frontline Education utilizes CSF as a hub to integrate the various standards, evaluate the overlap and ensure a single view of applying such standards to its computing environments. Frontline Education ensures its systems and environments are compliant with relevant laws, regulations or standards, including FERPA, HIPAA, CCPA, and SOC2, as applicable.

Student/teacher and/or principal data may be used for the following purposes:

- Frontline Education 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 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.

Third-party contractor data protection and security requirements: Third-party contractors shall ensure student/teacher and/or principal data that is shared with subcontractors, persons, or entities will adhere to applicable data protection and security requirements.

- Frontline Education requires that all service providers complete a risk assessment. Subsequent to the completion of a successful risk assessment, Frontline Education 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.

Data Retention:

- Frontline Education will not knowingly retain PII beyond the time required to support authorized educational/school purposes. Following termination or deactivation of a District 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 District shall be deleted promptly. Frontline Education may maintain

anonymized or aggregated data, including usage data, for analytics purposes to improve products and services.

Questions regarding the accuracy of student/teacher and/or principal data:

- To review or update your information to ensure its accuracy or to correct any errors and omissions, please contact your Educational Organization directly. Requests sent to Frontline Education seeking a copy of such records or asking that Frontline modify or delete any records that it maintains will be forwarded directly to the appropriate Educational Organization. Please note that even when records are modified or deleted from Frontline's active databases, copies may remain in data backups as necessary to comply with business or regulatory requirements.

Data storage and encryption practices:

- Frontline Education 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 FDE ("Full Disk Encryption") and all database backups are AES-256 encrypted.
- Frontline Education 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 Education 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.

Measures re identifying breaches and unauthorized disclosures:

- conduct an investigation and provide Educational Organization 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. The communication to the Educational Organization shall be made upon confirmation of the breach, without undue delay, to affected clients. Notifications to affected clients of material third-party breaches shall be made pursuant to legal and contractual requirements.

How training re federal and state laws governing confidentiality shall be provided and how third-party contractor ensures individuals will abide by data security and protection requirements:

- Such training shall be provided, and agreed to, at least annually via an online learning management system.