



MASTER SERVICES AGREEMENT

This Master Services Agreement is made effective as of the date of the signature below (the “Effective Date”) by and between Frontline Technologies Group LLC dba Frontline Education, with an address at 1400 Atwater Drive, Malvern, PA 19355 (“Frontline”), and the customer identified below (“Customer”). Frontline and Customer are sometimes referred to herein, individually, as a “Party” and, collectively, the “Parties.”

Customer is a municipal corporation with authority under Section 1950 of the New York Education Law to enter into, and enforce, contracts, and to provide cooperative educational services to school districts in New York State pursuant to cooperative educational service agreements (“CoSers”) approved by the New York State Education Department. Customer provides shared computer services, software, and technical training and support to school districts that enter into applicable CoSers (“participating school districts”).

Frontline licenses certain software products designed to support school operations and wishes to take advantage of Customer’s established relationships with school districts to introduce such software products to school districts in Customer’s service area, and to make such software products available to participating school districts with Customer’s support.

Customer wishes to make such software products available to school districts in Customer’s service area upon the commercial terms set forth herein and is willing to provide training and other technical support for such software products.

Accordingly, the parties have entered this Agreement to set forth the terms upon which such software products will be made available to participating school districts by Customer. The Effective Date of this Agreement will be the date it has been executed by both Parties.

By signing below, the Parties agree to be legally bound by the Terms and Conditions contained herein (the “Terms and Conditions”), including any exhibits and Purchase Orders entered into under these Terms and Conditions (collectively, this “Agreement”). This Agreement constitutes the complete and exclusive statement of the agreement between the Parties with respect to the software products described in the Agreement and any other software, products or other services provided by Frontline or any of its affiliates or predecessors prior to the Effective Date. For the avoidance of doubt, this Agreement supersedes any and all prior oral or written communications, proposals, RFPs, contracts, and agreements (including all prior license and similar agreements) and the Parties hereby terminate any such agreements. This Agreement supersedes any online terms of service or other online licenses or conditions on use of the software products described herein when those software products are used by Customer or a participating school district. In the event of a conflict between the provisions of the Terms and Conditions and the provisions of any Purchase Order, the Terms and Conditions shall govern.



<p>Frontline Technologies Group LLC dba Frontline Education</p> <p>Signature: <u><i>Scott Crouch</i></u></p> <p>Name: <u>Scott Crouch</u></p> <p>Title: <u>VP Financial Operations</u></p> <p>Address: <u>1400 Atwater Drive,</u> <u>Malvern, PA. 19355</u></p> <p>Email: <u>billing@frontlineed.com</u></p> <p>Date: <u>9/18/2024</u></p>	<p><u>Ulster BOCES</u> (Customer)</p> <p>Signature: <u><i>John Schinke</i></u></p> <p>Name: <u>Mr. John Schinke</u></p> <p>Title: <u>District Superintendent</u></p> <p>Address: <u>175 Rt 32N.</u> <u>New Paltz NY 12561</u></p> <p>Email: _____</p> <p>Date: <u>8/21/24</u></p>
--	--

Attached: *Terms and Conditions of Agreement*

- Exhibits:**
- Exhibit A: Customer Order Form
 - Exhibit B: Cost Schedule
 - Exhibit C-1: List Rates
 - Exhibit D-1: Implementation Fees
 - Exhibit D-2: Professional Services Fees

IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

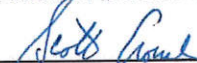
As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

Signature: 

Print Name: Scott Crouch

Title: VP Financial Operations

Company Name: Frontline Technologies Group LLC d/b/a Frontline Education

Date: 8/9/2024



PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law §2-d, Ulster BOCES wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
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 for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or 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:

Ulster BOCES
175 Route 32 North
New Paltz, New York 12561

or

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234

Complaints may also be directed to the
Chief Privacy Officer (CPO) via e-mail at
CPO@mail.nysed.gov


6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data as well as teacher or principal data.

Supplemental Information Regarding Third Party Contractors

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used by third party contractor;
2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.
6. Address how the data will be protected using encryption while in motion and at rest.

Signature: 

Print Name: Scott Crouch

Title: VP Financial Operations

Company Name: Frontline Technologies Group LLC d/b/a Frontline Education

Date: 8/9/2024

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Frontline Technologies Group LLC d/b/a Frontline Education (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Ulster County BOCES ("BOCES") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that Ulster County BOCES' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster County BOCES. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of Ulster County BOCES as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of Ulster County BOCES 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with Ulster County BOCES policy(ies) on data security and privacy. Contractor shall promptly reimburse Ulster County BOCES for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of Ulster County BOCES' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster County BOCES' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees 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;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to Ulster County BOCES, transitioned to a successor contractor, at Ulster County BOCES' option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Ulster County BOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

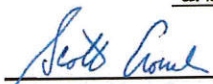
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, BOCES board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of Ulster County BOCES' Parent Bill of Rights.

NAME OF PROVIDER: Frontline Technologies Group LLC
d/b/a Frontline Education

BY: 

DATED: 8/9/2024

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

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.

Data Security and Privacy Plan Template

Version 1.0

Table of Contents

1. Purpose	2
2. Terminology.....	2-3
3. Relevant Laws, Regulation, Policies and Standards.....	3-4
1. <i>Family Education Rights and Privacy Act (FERPA)</i>	4
2. <i>New York Education Law§ 3012-c(10)</i>	4
3. <i>New York State Education Law§2-d</i>	4-5
4. Privacy, Confidentiality, and Internal Controls.....	5-8
5. Incident Response Plan Subcontractors.....	8
6. Subcontractors.....	9-10

1.0 Purpose

The purpose of this Data Security and Privacy Plan is to document Frontline Technologies Group LLC d/b/a Frontline Education ("hereinafter "Frontline Education") commitment and approach to protecting Confidential Information (as defined in Section 2.0 of this plan), and how it will handle any incidents where there is a breach or unintended disclosure of Confidential Information or a System (as defined in Section 2.0 of this plan) that supports it.

2.0 Terminology

Application - means Frontline Education's software that performs a user-facing function, such as a web application.

Confidential Information or Data - means any personally identifiable information related to students, student families/guardians, local education agency (LEA) employees, agents and/or volunteers obtained by or furnished to the Vendor; all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine readable form; and all information marked "confidential" by the LEA. Confidential Information includes, but is not limited to, names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, and any other information that constitutes "personally identifiable information" as defined in or pursuant to the Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 C.F.R. Part 99) (collectively, "FERPA"), or "personally identifying information" as defined or used in New York Education Law 3012-c.

Frontline Education may not disclose Confidential Information except to the extent such Confidential Information is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Vendor, (ii) demonstrated to have been known to the Vendor prior to disclosure by or through the LEA, (iii) disclosed with the prior written approval of the LEA, (iv) demonstrated to have been independently developed by the Vendor without reference to the Confidential Information, (v) disclosed to the Vendor by a third party under conditions permitting such disclosure, and/or (vi) disclosed as required by court order, subpoena, other validly issued administrative or judicial notice or order and/or as a matter of applicable law; provided, however, that in the event disclosure is required of the Vendor under the provision of any law or court order, the Vendor will (a) promptly notify the LEA of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the LEA to seek a protective order, and (b) disclose such Confidential Information only to the

extent allowed under a protective order, if any, or necessary to comply with the law or court order.

Notwithstanding the previous sentence, **Frontline Education** shall not disclose any "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2-d and its implementing regulations (8 NYCRR Part 121), or "personally identifying information" as defined or used in New York Education Law §3012-c to any other party without the prior written consent of the parent or eligible student except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the LEA; or unless required by statute or court order and **Frontline Education** has provided a notice of disclosure to the department, LEA board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by statute or court order.

FERPA - means the Family and Educational Rights and Privacy Act (20 U.S.C. §1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

Handle -means (in the context of Confidential Information) to create, view, modify, store, transmit or delete.

Local Education Agency (LEA) - means a school district or an educational service agency (e.g. BOCES, RIC).

PII - means personally identifiable information, as defined under FERPA.

System - means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

Vendor - means Frontline Technologies Group LLC, also known as **Frontline Education**

3.0 Relevant Laws, Regulation, Policies and Standards

3.1 Family Education Rights and Privacy Act (FERPA)

FERPA is the primary federal legislation that governs the privacy of educational records. The Vendor must hold all PII obtained, learned or developed by the Vendor in confidence pursuant to applicable provisions of FERPA. The Vendor understands that the release of PII to persons or agencies not authorized to receive such information is a violation of US federal law. Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to return PII to the LEA, when no longer needed or at the expiration of any contract. Vendor understands that upon request, it must permit the LEA access to PII that it

holds, in order for the LEA to meet other obligations under FERPA or pursuant to law.

3.2 New York Education Law § 3012-c(10)

New York Education Law § 3012-c(10) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Vendor understands that to the extent that information protected under New York State Education Law § 3012-c(10) is shared with Vendor, Vendor is responsible for complying with this law. Vendor further understands that New York State Education Law § 2-d imposes additional requirements concerning the confidentiality of teacher and principal evaluation data.

3.3 New York State Education Law § 2-d

New York State Education Law § 2-d imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law § 3012-c(10), including a number of requirements and obligations that apply directly to Vendor. Vendor understands that it is required to comply with the requirements of New York Education Law § 2-d and its implementing regulations (8 NYCRR Part 121), which require Vendor to:

- Limit internal access to Confidential Information covered under Education Law § 2-d ("Covered Confidential Information") to those employees or subcontractors that need access to provide the contracted services;
- Not use Covered Confidential Information for any other purposes than those explicitly authorized in the contract;
- Not disclose Covered Confidential Information to any other party without the prior written consent of the parent or eligible student, except to authorized representatives of the Vendor to the extent they are carrying out the contract and in compliance with state and federal law, regulations, and the contract, or unless required by statute or court order and the Vendor provides a notice of disclosure to Ulster County BOCES no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order;
- Maintain reasonable technical, administrative and physical safeguards to protect the security, confidentiality and integrity of Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified

under HIPAA by the US Department of Health and Human Services;

- . Notify the LEA of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse LEA for the full notification cost;
- . Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

Vendor also agrees to cooperate with the LEA in complying with the regulations implementing New York Education Law§ 2-d (i.e. 8 NYCRR Part 121) and any LEA or state policies promulgated pursuant to New York Education Law§ 2-d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Vendor's contract with the LEA,(b) its compliance with the LEA's Data Security and Privacy Policy, (c) its compliance with and signature of the Parent Bill of Rights required of the LEA, and (d) the inclusion of supplemental information concerning Vendor's contract in the Parent Bill of Rights. Vendor acknowledges that it has been provided access to the LEA's Data Security and Privacy Policy and has reviewed the same.

4.0 Privacy, Confidentiality, and Internal Controls

Frontline Education will:

- A. Comply with LEA's Data Security and Privacy Policy, in addition to all laws, regulations, policies and standards listed in Section 3.0 of this Data Security and Privacy Plan by:
 - 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.
- B. Hold Confidential Information in strict confidence, limit internal access to it to those employees or subcontractors that need access to provide the contracted services (via administrative processes and Application and System authentication mechanisms), and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon with the LEA;
- C. Provide training on federal and state law governing Confidential Information to any officers, employees, or assignees prior to them having access to Confidential Information

- Training shall be provided, and agreed to, at least annually via an online training management system
- D. Use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System, that will involve at least the following best practice technology approaches:
- 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.
- E. Protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer;
- F. Maintain all copies or reproductions of Confidential Information with the same security it maintains the originals, and at the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by the LEA, will destroy such Data, making it unusable and unrecoverable, except that backup files made in the normal course of business which may be retained per Frontline Education's data retention policy, for regulatory compliance; and
- G. Ensure Confidential Information will not appear in URLs of any Application.
- H. When the Agreement terminates between the LEA and Frontline Education, Frontline Education shall return such data to the LEA or if agreed to by the LEA, destroy the data that Frontline Education still maintains in any form in a manner agreeable to the LEA, except that backup files made in the normal course of business which may be retained per Frontline Education's data retention policy, for regulatory compliance.

Frontline Education will:

- A. Comply with LEA's Data Security and Privacy Policy, in addition to all laws, regulations, policies and standards listed in Section 3.0 of this Data Security and Privacy Plan by:
- 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.
- B. Hold Confidential Information in strict confidence, limit internal access to it to those employees or subcontractors that need access to provide the contracted services (via administrative processes and Application and System authentication mechanisms), and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon with the LEA;
- C. Provide training on federal and state law governing Confidential Information to any officers, employees, or assignees prior to them having access to Confidential Information
- Training shall be provided, and agreed to, at least annually via an online training management system
- D. Use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System, that will involve at least the following best practice technology approaches:
- 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.
- E. Protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer;
- F. Maintain all copies or reproductions of Confidential Information with the same security it maintains the originals, and at the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by the LEA, will destroy such Data, making it unusable and unrecoverable, except that backup files made in the normal course of business which may be retained per Frontline Education's data retention policy, for regulatory compliance; and

G. Ensure Confidential Information will not appear in URLs of any Application.

H. When the Agreement terminates between the LEA and Frontline Education, Frontline Education shall return such data to the LEA or if agreed to by the LEA, destroy the data that Frontline Education still maintains in any form in a manner agreeable to the LEA, except that backup files made in the normal course of business which may be retained per Frontline Education's data retention policy, for regulatory compliance.

5.0 Incident Response Plan

In the event an incident occurs where there is a breach or unintended disclosure of Confidential Information or a System that supports it, Frontline Education will adhere to this Incident Response Plan.

- A. Frontline Education will comply with all applicable breach notification laws, including New York State Education Law§ 2-d, Part 121 of the Commissioner's Regulations, and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law§ 208, as appropriate).
- B. Frontline Education will promptly notify the LEA in the most expedient way possible and without unreasonable delay but no more than 72 hours of the discovery of a breach or unintended disclosure of Confidential Information or a System that supports it. Such notification shall be by email and either certified mail, return receipt requested, or overnight mail.
- C. Frontline Education must cooperate with the LEA and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Information.

Response actions to incidents that might affect Confidential Information or Systems will be conducted quickly and with ample resources. Frontline Education will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.

Frontline Education will provide the LEA with the opportunity to view all incident response evidence, reports, communications and related materials, if they so request.

- E. If requested by the LEA, or if required by law, Frontline Education will notify in writing all persons affected by the incident, at its own cost and expense and/or pay for or promptly reimburse the LEA for the full costs of any notifications required by law as a result of a breach or unauthorized release attributed to Frontline Education

6.0 Subcontractors

Frontline Education (**choose one: will**) utilize subcontractors. In the event that Frontline Education utilizes subcontractors to support a System that Handles Confidential Information (each a "subcontractor") to provide the contracted services, Frontline Education shall ensure that any such subcontractor will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law §2-d) that are imposed on Frontline Education **by** 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.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Ulster County BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the LEA enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include supplemental information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract;
2. How the third party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements;
3. The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the agreement (e.g., whether, when and in what format it will be returned to Ulster County BOCES, and/or whether, when and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated;
6. How the data will be protected using encryption while in motion and at rest.

The Supplemental Information elements listed above have been developed for the contract between Ulster County BOCES and the Company and are hereby incorporated by reference into this Data Security and Privacy Plan.

The Company shall:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Ulster County BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Ulster County BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

Company hereby acknowledges that it is aware of and agrees to abide by the terms of the Ulster County BOCES' Parents Bill of Rights for Data Privacy and Security.

SIGNATURE: Scott Crouch

PRINTED NAME: Scott Crouch

TITLE: VP Financial Operations

COMPANY NAME: Frontline Technologies Group LLC d/b/a Frontline Education

DATE: 8/9/2024