

Addendum D

Parents Bill of Rights for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The District's Bill of Rights will state in clear and plain English terms that:

- a. A student's personal identifiable information (PII) cannot be sold or released for any commercial purposes;
- b. Parents have the right to inspect and review the complete contents of their child's education record;
- c. State and federal laws protect the confidentiality of PII, 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;
- d. A complete list of all student data elements collected by the state is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234; and
- e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>. Parents can also send their written complaint to the Sullivan BOCES Data Protection Officer at 15 Sullivan Avenue, Suite 1, Liberty New York 12754

Addendum E

PARENTS' BILL OF RIGHTS - SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by (the "Vendor") are limited to the purposes authorized in the contract between the Vendor and Sullivan County BOCES (the "BOCES") dated 10/31/23 (the "Contract Date").
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to 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., Family Educational Rights and Privacy Act ("FERPA"); Education Law § 2-d; 8 NYCRR § 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in: (choose one)

<input type="checkbox"/>	The agreed upon format to BOCES (or)
<input checked="" type="checkbox"/>	Will be destroyed by the Vendor as directed by the BOCES. Backup files made in the normal course of business may be retained per Vendor's data retention policy, for regulatory compliance.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the BOCES in a Vendor's product and/or service by following the BOCES's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by BOCES in Vendor's product and/or service by following the appeal procedure in the BOCES's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the BOCES will be stored (United States. 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.). The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum F

VENDOR'S DATA SECURITY AND PRIVACY PLAN

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.**

DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Sullivan County _____ BOCES (hereinafter "BOCES") and Frontline Technologies Group, LLC d/b/a Frontline Education _____ (hereinafter "Contractor") entered into an agreement dated _____ October 31, 2023 _____ (hereinafter "Agreement") for IEP Direct, Analytical Services, 504 Plans, ESA (BOCES Direct) _____ (hereinafter "Services").

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the BOCES.

1. During the term of the Agreement Contractor will implement all state, federal and local data security and privacy requirements, consistent with the BOCES Data Security and Privacy Policy in the following way(s):

- 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.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

- 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. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the BOCES Parents Bill of Rights for Data Privacy and Security and will comply with same.

- a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
 - b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.
-
- c. At the end of the term of the Agreement, Contractor will destroy, transition, and/or return all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement except that backup files made in the normal course of business which may be retained per Contractor's data retention policy, for regulatory compliance.
 - d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

- e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided:

Frontline shall provide such training, and such training shall be agreed to, at least annually via an online learning management system.

5. Subcontractors (check one):

☐ Contractor shall not utilize subcontractors.

☒ Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: *Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the BOCES.*

Investigate and provide BOCES 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 BOCES 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.

7. Termination of Agreement. Within ____ days of termination of the Agreement, Contractor shall return all data to the BOCES and (chose one):

☒ Delete or destroy all student data or teacher or principal data in its possession, except that backup files made in the normal course of business which may be retained per Contractor's data retention policy, for regulatory compliance.

☐ Transition all data to a successor contractor designated by the BOCES in writing using _____.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security

and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

AMENDMENT

THIS AMENDMENT entered into on October 31, 2024 amends the Software License Vendor Agreement dated October 31, 2023 entered into by and between the Sullivan County BOCES ("BOCES") and Frontline Technologies Group LLC ("Vendor") ("Agreement").

WHEREAS, the Agreement expires on October 31, 2024; and

WHEREAS, BOCES and Vendor desire to extend the term of the Agreement as reflected herein.

NOW THEREFORE, for valuable consideration the Parties hereto amend the Agreement as follows:

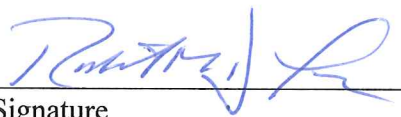
1. **Term.** The Term of the Agreement is hereby extended for one (1) year, such that the Term shall expire on October 31, 2025.

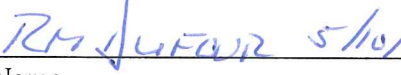
2. **Conflict.** In the event of a conflict between the terms of this Amendment and the terms of the Agreement, the terms of this Amendment shall control. All of the defined terms in the Agreement shall have the same definitions in this Amendment, unless otherwise defined herein.

3. Except as expressly set forth in this Amendment, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment as of the date first set forth above.

SULLIVAN COUNTY BOCES


Signature


Name

VENDOR


Signature

May 7, 2024
Name