Exhibit E: 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.

EXHIBIT F

DATA SHARING AND CONFIDENTIALITY AGREEMENT INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND SUPPLEMENTAL INFORMATION

1. Purpose

a. This Appendix and Data Sharing and Confidentiality Agreement ("Agreement") supplements any agreement between the parties and is intended to conform to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Appendix consists of the terms of this Data Sharing and Confidentiality Agreement, and Exhibit A which is a copy of Onondaga-Cortland-Madison (OCM) BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information that is required to be posted on Onondaga-Cortland-Madison (OCM) BOCES' website. Exhibit A is attached hereto and incorporated by reference.

b. To the extent that any terms contained within the bidding documents, or any terms contained within any other written agreement between the parties, conflict with the terms of this Appendix, the terms of this Appendix will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of these bidding documents to the extent that any term of the TOS conflicts, the terms of this Appendix will apply and be given effect.

2. Definitions

a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b. "Commercial Purpose" or "Marketing Purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.

c. "Disclose" or "Disclosure" means to permit access to, or the release, transfer, or other communication of Personally Identifiable Information (as defined below) by any means, including oral, written, or electronic, whether intended or unintended.

d. "Education Records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

e. "Eligible Student" means a student who is eighteen years or older.

f. "Encryption" means methods of 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.

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

h. "Personally Identifiable Information," as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).

i. "Release" shall have the same meaning as Disclosure or Disclose.

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

k. "Student data" means Personally Identifiable Information from the student records of an educational agency. For purposes of this Agreement, "student data" includes information made accessible to Vendor by OCM BOCES, OCM BOCES officers, OCM BOCES employees, OCM BOCES agents, OCM BOCES students, and/or the officers, employees, agents, and/or students of educational agencies with whom OCM BOCES contracts.

l. "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this Agreement, "student data" includes information made accessible to Vendor by OCM BOCES, OCM BOCES officers, OCM BOCES employees, OCM BOCES agents, OCM BOCES students, and/or the officers, employees, agents, and/or students of educational agencies that contract with OCM BOCES in order to access Vendor's services.

m. "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

n. "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of these bid documents. For purposes of this Appendix, the term also includes BOCES or any other BOCES that is licensed to use Vendor's Product pursuant to these bid documents to support its own educational programs or operations.

3. Confidentiality of Protected Data

a. Vendor acknowledges that the Student Data and Teacher or Principal Data (collectively, "Protected Data") it receives pursuant to these bid documents may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

b. Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and any applicable BOCES' policy on data security and privacy. Vendor acknowledges BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of an award to a successful bidder under these bid documents. BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption,

and Vendor and BOCES agree to engage in good faith negotiations to modify this Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

c. Protected Data received by Vendor shall not be sold or used for marketing purposes.

d. The exclusive purpose for which Vendor is being provided access to Personally Identifiable Information is to provide Transportation Logistics and Communication Software. Vendor does not monitor or use customer content for any reason other than as part of providing our services.

4. Data Security and Privacy Plan

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

a. In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Agreement, consistent with BOCES' data security and privacy policy, Vendor shall perform as follow:
   - Vendor's policies and practices shall comply with state, federal and local data security and privacy requirements.
   - Vendor shall limit access and protect data exchanged under this Agreement using industry best-practices.
   - Vendor shall regularly review all laws and data security agreement and contracts to ensure continuous compliance with this Agreement.

b. In order to protect the security, confidentiality and integrity of the Protected Data that it receives, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the agreement between the parties:
   - Vendor's hosted solution is backed by Amazon Web Servers ("AWS"). Vendor shall only utilize AWS regions within the United States to store data produced in the United States.
   - Vendor shall protect data using best practice technologies including but not limited to using firewalls, virus protection, password protection, NTFS file permissions, encryption, patch and vulnerability management and modern operating systems.
   - Vendor shall ensure data in transit and at rest is encrypted.

c. Vendor will comply with all obligations set forth in BOCES' "Supplemental Information" as set forth below.

d. For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows:
   - Vendor shall limit access to data under this Agreement to only those involved in providing services under this Agreement.
   - Vendor shall provide annual training to its Client Services team in all data protection policies. Violations of Vendor's Data Security policies are grounds for disciplinary action including but not limited to dismissal from employment.

e. Vendor will utilize sub-contractors for the purpose of fulfilling one or more of its obligations under these bid documents. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under these bid documents, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES' "Supplemental Information" below.

f. Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 5 below.

g. Upon expiration or termination of any agreement between the parties without a successor agreement in place and upon request, Vendor shall assist OCM BOCES and any Participating Educational Agency for the provision of Vendor's services in exporting any and all Protected Data previously received by Vendor back to OCM BOCES or the Participating Educational Agency that generated the Protected Data. Vendor shall thereafter securely delete or otherwise destroy any and all Protected 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 of such data) as well as any and all Protected Data maintained on behalf of Vendor in secure data center facilities. Backup files made in the normal course of business may be retained per Vendor's data retention policy, for regulatory compliance Vendor shall ensure that no copy, summary, or extract of the Protected Data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities, except that backup files made in the normal course of business may be retained per Vendor's data retention policy, for regulatory compliance. Any and all measures related to the extraction, transmission, deletion, or destruction of Protected Data will be completed within six (6) months of the expiration/termination of the agreement between OCM BOCES and Vendor (or sooner, upon request), and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Vendor may continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they 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 OCM BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be considered a breach including a breach of the terms of this Agreement:

a. Limit internal access to Protected Data to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

b. Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under these bid documents.

c. Not use Protected Data for any purposes other than those explicitly authorized in this Agreement.

d. Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

e. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

g. Provide notification to Onondaga-Cortland-Madison (OCM) BOCES (and Participating Educational Agencies), of any breach of security resulting in an unauthorized release of Protected Data 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, but not more than seven (7) calendar days after discovery of the breach;

h. Where a breach or unauthorized release of Protected Data is attributable to Vendor, Vendor will pay or reimburse OCM BOCES and/or any Participating Educational Agencies for the full cost of any notifications OCM BOCES and/or such other Participating Educational Agencies is/are required to make by applicable law, rule, or regulation; and

i. Vendor will cooperate with OCM BOCES, any Participating Educational Agency, and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

6. Notification of Breach and Unauthorized Release

In the event of a data security and privacy incident implicating the Protected Data of OCM BOCES or Participating Educational Agencies:

a. Vendor shall work to mitigate the incident and provide notification.

b. Vendor will notify OCM BOCES, and any Participating Agency, of any such incident in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and the provisions contained herein and in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

c. Vendor will cooperate with Onondaga-Cortland-Madison (OCM) BOCES and Participating Agency and provide as much information as possible directly about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information

involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

d. Vendor acknowledges that upon initial notification from Vendor, Onondaga-Cortland-Madison (OCM) BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Onondaga-Cortland-Madison (OCM) BOCES, Vendor will promptly inform OCM BOCES in writing.

e. Vendor will consult directly with OCM BOCES prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

7. Miscellaneous

a. The terms of this Agreement, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Vendor's terms of service or privacy policy.

b. If any provision of this Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision to this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

c. This Agreement shall be governed by the laws of the State of New York. The Parties hereto agree that exclusive venue for any litigation, action or proceeding arising from or relating to this Agreement shall lie in the state and federal courts located in Onondaga County, New York, and the Parties expressly waive any right to contest such venue for any reason whatsoever.

In witness of the foregoing, the duly authorized representatives of the Parties have executed this Agreement as of the date both parties have signed below.

FRONTLINE TECHNOLOGIES GROUP, LLC

By: Scott Crouch
Name: Scott Crouch
Title: VP Financial Operations
Date: 9/11/2024

OCM BOCES

By: Suzanne Slack
Name: Suzanne Slack
Title: Assistant Superintendent for Administration
Date: 08 / 29 / 2024