



To our valued New York Clients:

Frontline Education provides special education, student health, Medicaid and other software and services to over 800 school districts in the State of New York for whom we store student, teacher, and administrator Personally Identifiable Information (PII) and Personal Health Information (PHI). We are committed to safely and securely storing PII and PHI in accordance with federal law (FERPA) and New York state education law (New York Ed. Law 2-d) and appreciate your trust in us.

During the recent school year, Frontline Education has been overwhelmed by individual districts requesting that we execute Data Privacy Agreements, ostensibly requiring us to meet these legal requirements but with different, and in most instances, inconsistent provisions. Frontline Education has developed the attached New York Education Law 2-d Rider and attachments which describes how our systems meet the legal obligations of both FERPA and NY Ed. Law 2-d. We ask that you accept these as fulfillment of the New York Education Law 2-d requirements in lieu of a separate Data Privacy Agreement.

If you have any questions, please contact the Frontline Legal Department at [Legal@FrontlineEd.com](mailto:Legal@FrontlineEd.com).

## 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 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 School District ("DISTRICT") and Frontline Technologies Group LLC dba Frontline Education ("CONSULTANT") to the contrary, CONSULTANT agrees as follows:

CONSULTANT 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 CONSULTANT uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. CONSULTANT 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. CONSULTANT 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, CONSULTANT shall have in place sufficient internal controls to ensure that the DISTRICT's and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act, Family Educational Rights and Privacy Act ("FERPA") and Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 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 the DISTRICT and/or a Participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the DISTRICT and/or its Participants as that term is defined in §99.3 of FERPA,

-AND-

Personally identifiable information from the records of the DISTRICT and/or its Participants 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.”

CONSULTANT 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, CONSULTANT agrees to comply with the DISTRICT policies on data security and privacy. CONSULTANT shall promptly reimburse DISTRICT or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by CONSULTANT, its subcontractors, or assignees. In the event this Agreement expires, is not renewed or is terminated, CONSULTANT shall return, by secure transmission, or securely destroy all of DISTRICT or its Participants’ data, including any and all Protected Data in its possession.

### **Data Security and Privacy Plan**

CONSULTANT or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of DISTRICT’s and/or its Participants’ Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of DISTRICT’s Parents’ Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to CONSULTANT’s possession and use of Protected Data pursuant to the Agreement.
2. An outline of how all State, Federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the CONSULTANT’s policy on data security and privacy.
3. An outline of the measures taken by CONSULTANT to secure Protected Data and to limit access to such data to authorized staff.
4. An outline of how CONSULTANT will use “best practices” and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.
5. An outline of how CONSULTANT will ensure that any subcontractors, persons or entities with which CONSULTANT will share Protected Data, if any, will abide by the requirements of CONSULTANT’s policy on data security and privacy, and the contractual obligations with respect to Protected Data.

(1) The New York parents bill of rights for data privacy and security (“Parents Bill of Rights”) is incorporated into the Agreement. Such Parents Bill of Rights is set forth at Exhibit A.

(2) Internal access to DISTRICT’s education records shall be limited to those individuals that CONSULTANT reasonably determines have a legitimate educational interest;

(3) CONSULTANT shall not use DISTRICT education records for any other purposes than those explicitly authorized by this Agreement.

(4) CONSULTANT shall not disclose any personally identifiable information from DISTRICT education records to any third parties except:

a. To subcontractors of CONSULTANT to the extent such personally identifiable information is reasonably necessary to carry out this Agreement.

b. To a successor entity pursuant to a merger, consolidation or sale of substantially all of its assets of CONSULTANT provided that such successor shall continue to be bound to the obligations of the Agreement.

c. With the prior written consent of the applicable parent or eligible student; or

d. If such disclosure is required by statute or court order and CONSULTANT provides notice of such disclosure to DISTRICT no later than the time the information is disclosed unless CONSULTANT is prohibited by statute or court order from making such disclosure to DISTRICT.

(5) CONSULTANT shall maintain reasonable administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of District personally identifiable student information in its custody. Without limiting the foregoing, such safeguards shall comply with applicable federal and state laws and align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

(6) CONSULTANT shall use encryption technology designed to protect student, teacher or principal personally identifiable information while in motion or in CONSULTANT's custody from unauthorized disclosure.


(7) CONSULTANT shall notify such District of any breach of security resulting in an unauthorized release of such student, teacher or principal personally identifiable information that CONSULTANT or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of District and/or contractual obligations binding on the CONSULTANT relating to data privacy and security, in the most expedient way reasonably possible and without unreasonable delay. If notification to a parent, eligible student, teacher or principal is required under this Subsection 7 due to the unauthorized release of student data by CONSULTANT or its assignee, CONSULTANT shall be responsible for reimbursing District for the cost of such notification.

1. Attached as Exhibit "A" is a copy of Parent's Bill of Rights for Privacy and Security.
2. Attached as Exhibit "B" is a copy of the CONSULTANT's Data Privacy and Security Plan.

**Third-Party Acknowledgement**

As a third-party contractor, I acknowledge that our contract with the School District may necessitate the receipt of student data, and as such, requires adherence with NY State Education Law §2-d and the District's Parents' Bill of Rights for Data Privacy and Security. In this regard, we acknowledge our responsibility to adhere to the document as applicable to the services we provide and have instituted processes to abide by same.

**FRONTLINE TECHNOLOGIES GROUP LLC dba Frontline Education**

By: 

Position: Vice President

Date: 3/12/20

## EXHIBIT "A"

### PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents and guardians of students attending school in the School District are advised that they have the following rights with regard to student data:

- (1) Student data will not be released or sold by the School District for commercial purposes.
- (2) A parent or guardian has the right to inspect and review the complete contents of his or her child's education record.
- (3) State and Federal law protect the confidentiality of personally identifiable information. The District utilizes the following safeguards to protect personally identifiable information: encryption, password protection, confidential information is destroyed in accordance with approved records schedules, etc.
- (4) A list of all student data elements collected by New York State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> or by writing to Office of Information & Reporting Services, New York State Education Department, Room 86E EBA, 89 Washington Avenue, Albany, New York 12234.
- (5) Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to: New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

This Bill of Rights will be included with every contract entered into by the District with an outside contractor if the contractor will receive student data or teacher or principal data.

This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student data or teacher or principal data, including the exclusive purposes for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.



Exhibit B  
Frontline Education  
Data Security and Privacy Plan

Frontline Technologies Group LLC, doing business as Frontline Education, has established a unified control framework based on the NIST Cyber Security Framework (CSF). Frontline Education has several security control standards that are applicable to our product development and our operations environments. The CSF, as our primary standard allows us to use it as a hub where we can integrate the various standards, evaluate the overlap, and ensure we have a single view of applying those standards to our computing environments. We ensure our systems and environments are compliant with relevant standards, including PCI DSS and SOC2, as required.

**The exclusive purposes for which the student data or teacher or principal data will be used.**

- Frontline Education collects personally identifiable information (PII) on individuals including administrators, educators, and students, and others as outlined in the Frontline Technologies Group LLC Privacy Policy.
- Frontline Education will only use PII as specifically permitted in the agreements we maintain with our customers. Specifically, PII is used for the provision of services and tracking of information across our products and platforms.
- Frontline Education may use de-identified, anonymized, and aggregated data for various purposes including improving the customer experience and refining and developing additional products and services.

**How the third-party contractor will ensure that the subcontractors, persons, or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.**

- Frontline Education requires that all service providers we use go through a risk assessment. We then qualify their products/services for use based on their need to interact with customer data. We require a SOC2 (or comparable) independent audit of their operations at least every six months.

**When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.**

- Frontline Education will not knowingly retain personal information beyond the time period required to support the 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, but any and all Student Data associated with the District will be deleted promptly. We may maintain anonymized or aggregated data, including usage data, for analytics purposes.

**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.**

- 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 demanding 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.

**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, including whether such data will be encrypted.**

- Frontline Education encrypts data within our production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using 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 at least yearly.