

Exhibit H

EDUCATION LAW 2-d RIDER

This Exhibit H supplements the underlying Agreement to which it is attached to ensure that the underlying Agreement conforms to the requirements of New York State Education Law Section 2-d and related Regulations of the Commissioner of Education ("Section 2-d"). To the extent that any term of the Agreement conflicts with the terms of this Exhibit, the terms of this Exhibit shall apply and be given effect.

As used in this Exhibit, the term "student data" means personally identifiable information, as defined in New York Education Law Section 2-d, from student records that Frontline receives from Customer or from a participating school district.

As used in this Exhibit, the term "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 New York Education Law Sections 3012-c and 3012-d.

As used in this Exhibit, the term "protected data" means student data and teacher or principal data

1. Frontline agrees that the security, confidentiality, and integrity of protected data shall be maintained in accordance with state and federal laws that protect the confidentiality of personally identifiable information, and also in accordance with Customer's Parents Bill of Rights for Data Security and Privacy, provided below.

2. Frontline agrees that, to the extent applicable, it will disclose protected data received from Customer or a participating school district only to those officers, employees, and agents who need access to provide the contracted services. Frontline further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Frontline who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data.

3. The exclusive purpose for which Frontline is being provided access to protected data is for providing Customer and its participating school districts with the functionality of the Products or Services accessed by each participating school district pursuant to a cooperative educational service agreements (CoSer) with Customer. Protected data received by Frontline, or by any assignee of Frontline, from Customer or a participating school district shall not be sold or used for marketing purposes.

4. The initial term of this Agreement expires on June 30, 2020 but the Agreement may be ~~automatically~~ extended for one or more 12-month periods. Upon expiration of this Agreement without a successor agreement in place, Customer may request that Frontline delete all protected data previously received from Customer or a participating school district that has not made alternative arrangements with Frontline to continue using Frontline Services. Frontline shall (at Customer's or the participating school district's expense) provide commercially reasonable support to Customer to extract data from Frontline Services in a format suitable for transfer to another service or platform.

5. In the event that a teacher or principal wishes to challenge the accuracy of teacher or principal data, they shall utilize the appeal process in the APPR Plan of their employing school district. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the student's district of enrollment for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

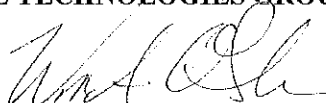
6. Student data transferred to Frontline by Customer or a participating school district will be stored in electronic format on systems maintained by Frontline or subcontractor of Frontline in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. Frontline will take measures aligned with industry best practices and the NIST Cybersecurity Framework and reasonably designed to protect the privacy and security of protected data while it is stored in such facility. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

7. Frontline acknowledge that it has the following obligations with respect to any protected data received from Customer or a participating school district and any failure to fulfill one of these statutory obligations shall be a breach of the underlying Agreement:

- limit internal access to education records to those individuals that are determined to have legitimate educational reasons in compliance with Section 2-d and FERPA;
- not use education records for any purpose other than those explicitly authorized in this Agreement;
- not disclose any personally identifiable information to any other party who is not an authorized representative of Frontline, Customer, or a participating school district using the information to carry out that Party's obligations under this Agreement, unless (1) that other party has the prior written consent of the parent or eligible student, or (2) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- use encryption technology that complies with New York Education Law Section 2-d and related Commissioner Regulations to protect data while in motion or in its custody from unauthorized disclosure;
- notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of student data by Frontline 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 no more than seven (7) calendar days after discovery of the breach; and
- ensure by contractual agreements or other legally binding measures that any subcontractor, assignee, or other agent (including any Hosting Service Provider) to whom Frontline discloses protected data will comply with the same data security and privacy standards required of Frontline under this agreement and applicable state and federal laws.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

FRONTLINE TECHNOLOGIES GROUP, LLC D/B/A FRONTLINE EDUCATION

BY: 

William A. O'Shea
Chief Financial Officers

DATED: May 11, 2023

**EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY**

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.
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.

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

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk 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 Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

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

Frontline Education's products are used by school districts and BOCES to achieve efficient and effective operations and the licensed products are only effective with the use of school data, including PII.

2. 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 does not share client data with any third-party contractors.

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

Upon expiration of this Agreement without a successor agreement in place, Customer may request that Frontline delete all protected data previously received from Customer or a participating school district that has not made alternative arrangements with Frontline to continue using Frontline Services. Frontline shall (at Customer's or the participating school district's expense) provide commercially reasonable support to Customer to extract data from Frontline Services in a format suitable for transfer to another service or platform.

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

Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

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, including whether such data will be encrypted.

Student data transferred to Frontline by Customer or a participating school district will be stored in electronic format on systems maintained by Frontline or subcontractor of Frontline in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. Frontline will take measures aligned with industry best practices and the NIST Cybersecurity Framework and reasonably designed to protect the privacy and security of protected data while it is stored in such facility. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

Third Party Contractors are required to:

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 Eastern Suffolk 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 Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.



EXHIBIT A: FRONTLINE PRIVACY POLICY

The privacy of the school districts and schools who purchase our Service (“Districts”), and to educators and students whose information we may access on behalf of a District (“Educators” and “Students”) is a high priority for Frontline Technologies Group LLC (“Frontline”).

Frontline provides a platform that provides Districts with the best, most popular tools for employee management, all in one place. Built specifically for K-12 districts, our tools help you get out of the administrative tasks and instead focus on advancing student growth through your employees. We also provide online tools for educators to discover job opportunities and an online marketplace where educators can buy, sell and share valuable classroom resources and educational materials. Educators and school administrators can then more efficiently manage administrative tasks and instead focus on advancing student growth through your employees. As we describe below, Districts decide which data are integrated with Frontline, and Districts are responsible for determining whether data are ever shared with Frontline.

Information We Collect

Information about Districts and Schools

We ask for certain information when a District administrator, Educator or other user registers with Frontline, or if the user corresponds with us online, which may include a name, school name, school district name, school email address account name, phone number, and/or message content. We may also retain information provided by a District or School if the District or Schools sends us a message, posts content to our website or through our Service, or responds to emails or surveys. Once a District begins using the Frontline Service, we will keep records of activities related to the Service. We use this information to operate, maintain, and provide the features and functionality of the Service, to monitor our Service offerings, and to communicate with our Districts and website visitors. Frontline stores data provided by Educational Organizations related to teachers and other school employees, such as:

- Demographic information including the individual’s name, address, email address, and date of birth, social security number;
- Credentials obtained and the granting institution;
- Information about the individual’s employment with the Educational Organization;
- System usernames and passwords.

Student Data

Frontline has access to personally identifiable information about students (“Student Data”) in the course of providing its services to a District. We consider Student Data to be confidential and do not use such data for any purpose other than to provide the



services on the District's behalf. Frontline receives Student Data only from the District and never interacts with the Student directly. Frontline has access to Student Data only as requested by the District and only for the purposes of performing Services on the District's behalf. The data your Educational Organization stores on Frontline's systems may include the following information about students and their guardians:

- Demographic information including name, mailing address, email address, and date of birth;
- Student education records including your student's grades, class enrollment, and behavioral records;
- Health-related information required for Medicaid reimbursement

Information Collected Through Technology

We automatically collect certain types of usage information when visitors view our website or use our service. We may send one or more cookies — a small text file containing a string of alphanumeric characters — to your computer that uniquely identifies your browser and lets Frontline help you log in faster and enhance your navigation through the site. A cookie may also convey information to us about how you use the Service (e.g., the pages you view, the links you click and other actions you take on the Service), and allow us to track your usage of the Service over time. We may collect log file information from your browser or mobile device each time you access the Service. Log file information may include anonymous information such as your web request, Internet Protocol ("IP") address, browser type, information about your mobile device, number of clicks and how you interact with links on the Service, pages viewed, and other such information. We may employ clear gifs (also known as web beacons), which are used to anonymously track the online usage patterns of our Users. In addition, we may also use clear gifs in HTML-based emails sent to our Districts to track which emails are opened and which links are clicked by recipients. The information allows for more accurate reporting and improvement of the Service. We may also collect analytics data, or use third-party analytics tools, to help us measure traffic and usage trends for the Service. We do not allow third party advertising networks to collect information about the users of our Site or Service. We use or may use the data collected through cookies, log files, device identifiers, and clear gifs information to: (a) remember information so that a user will not have to re-enter it during subsequent visits; (b) provide custom, personalized content and information; (c) to provide and monitor the effectiveness of our Service; (d) monitor aggregate metrics such as total number of visitors, traffic, and usage on our website and our Service; (e) diagnose or fix technology problems; and (f) help users efficiently access information after signing in.

Disclosure to Third Parties

We will not disclose the information described above to any third party unless we believe that such action is necessary to (a) comply with a court order or other legal process served on us or assist government enforcement agencies; (b) investigate or prevent



suspected illegal activities or protect the security and integrity of Frontline Education, Inc.; (c) enforce this Privacy Policy, our Terms of Service, or other such binding agreements; (d) take precautions against liability, investigate or defend against any third-party claims or allegations; or (e) exercise or protect the rights, property, or personal safety of Frontline, its employees, or customers.

Frontline only shares information in the ways described in this Privacy Policy. We never sell personal information to third parties. Frontline stores such information in its facilities, such as on servers co-located with third-party hosting providers. All third party vendors who have access to customer information due to services provided by Frontline are evaluated and must comply with the Privacy Policy prior to contracting with that vendor. Additionally, we review the ongoing security posture of our vendors through outside audit reporting (SOC 2, Type 2) and our own vendor risk analysis.

How We Protect Your Information

At Frontline, we have adopted the NIST Cybersecurity Framework as the model for our security program. We have organized our processes, organization and technology to support our strategic pillars for Prevention, Detection and Response. We have a dedicated security team aligned to these pillars and are continuously adjusting to new threats.

Prevention

Frontline maintains strict administrative, technical and physical procedures to protect information stored in our servers. Access to information is limited (through unique account credentials) to those employees who require it to perform their job functions. Additionally, we use unique account identifiers which attribute each user to a specific account and those accounts to specific organizations. We use industry-standard Transport Layer Security (TLS) encryption technology to safeguard the account registration process, sign-in information and data transmitted to Frontline servers. We store and process data in accordance with industry best practices. This includes appropriate safeguards to secure data from unauthorized access, disclosure, and use. We conduct periodic risk assessments to adjust to new threats and reallocate resources. We perform and remediate any identified security vulnerabilities in a timely manner. We protect customer passwords with a salted SHA-256, one-way cryptographic hash function. Frontline also follows a Secure Development Lifecycle which includes code review, quality and security testing and penetration testing. Frontline provides security and privacy training and awareness programs to all employees.

Detection

We have installed advanced endpoint detection and response technology which allows for “attack pattern” identification and records all system activity. These intelligent agents are identifying anomalous activities and producing alerts which go beyond simple anti-virus signature matching. Our team monitors and fine-tunes these rules for the latest threats and unusual activity. We also monitor application and database activity and use event management tools that actively correlate user actions and event data, then call attention to potential internal and external threats.



Response

We have a written incident response plan which includes response team training and periodic validation. We will notify, without unreasonable delay, the local or regional board of education of such breach of security once an investigation has been conducted to determine the nature and scope of such unauthorized release, disclosure or acquisition, and the identity the information involved.

Data Management

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 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. We 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.

Product Security Functions and Customer Responsibility

You can use several Frontline Education features to control the objects, fields, and specific data records to which your users have access. It is incumbent on the customer to use these features to design a roles-based security model that complies with your policies. Our applications provide fields and forms that allow for general purpose text and file attachment. This provides a way to capture information outside of standard fields. However, you should have a data classification policy and educate your users on how to handle sensitive data. This should apply to free form content fields and attachments in Frontline Education applications.

Despite these precautions, no system can be completely secure and there remains a risk that unauthorized access or use, hardware or software failure, human error, or a number of other factors may compromise the security of your information.

Marketing and Promotions

You may receive email communications for partner or internal promotions and you will always have the ability to opt out directly in the email message. Product related messages cannot be opted out of and will continue to keep you informed of important product updates. We do not use or disclose student information collected for behavioral targeting



of advertisements. Please remember that this privacy policy applies to the Frontline Services and Frontline website, and not other websites or third party applications, which may have their own Privacy Policies. You should carefully read the privacy practices of each third party application before agreeing to engage with the application through the Service.

Updates to this Privacy Policy

We may update or modify this Privacy Policy to reflect changes in the way Frontline maintains, uses, shares, or secures your information. Please check this Policy each time you interact with our systems to ensure that you are aware of any revisions. Prior to any material changes to this Policy becoming effective, Frontline will provide at least thirty (30) days' notice to your Educational Organization and allow it the opportunity to make choices regarding the data it stores with Frontline.

How to Contact Us

If you have questions about this Privacy Policy, please email: security@frontlineed.com

This privacy policy was last modified on February 2017.