frontline education

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

frontline education

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 alters 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.

frontline education

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.