EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms 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 Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit 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 the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information 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 or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "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 the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA 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 Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 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 the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

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 Erie 1 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 Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" 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: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor ___x___will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontactors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontactors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

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 a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records 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 the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality 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 under the MLSA, 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 that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data 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.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee 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, Erie 1 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 Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees 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.

EXHIBIT D (CONTINUED)

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(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.

(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.nysed.gov/data-privacy-security/student-data-inventory**, 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.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the 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/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Scott Crouch

Signature

Scott Crouch

Printed Name

Vice President

Title

7/2/20

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND *FRONTLINE EDUCATION*

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with *Frontline Education* which governs the availability to Participating Educational Agencies of the following Product(s):

Professional Learning Management
Employee Evaluation Management

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontactors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontactors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontactors, assignees, or other authorized agents abide by the provisions of these agreements by: *By contractually binding the parties to Education Law 2-d.*

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on _____ and expires on _____
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back

to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Privacy Policy

The privacy of the online visitors to our websites, of school districts and schools who purchase our products and services, of educators and students whose information we may receive on behalf of a customer, and of the individuals we otherwise interact with is a high priority for Frontline Technologies Group, LLC ("Frontline", "we", "us", or "our").

Frontline provides a platform that provides customers with the best, most popular tools for employee management, all in one place. Built specifically for K-12 school districts and educators, our tools help you get out of the administrative tasks and instead focus on advancing student growth through your employees. We also offer solutions for educators to develop professionally and find employment opportunities.

Information We Collect

Information about Districts and Schools: When districts and schools purchase and use our products and services, we receive certain information about them and their users. We receive information when a district's administrator, educator, or other district user registers with Frontline, or if the district user corresponds with us online. This information may include the individual's name, school name, school district name, school email address and/or account name and password, phone number, role at the district, state the district is located in, and/or message content. We may also receive information about districts from third parties. We may retain information provided by a district if a district user sends us a message, posts content to our website or through our services, or responds to emails or surveys. Once a district begins using our services, we will keep records of activities related to the services. We use the above information, or share this information with our service providers, to, among other things, operate, maintain, and provide the features and functionality of the services; to monitor our services offerings; to communicate with our districts and website visitors; and promote our products and services to districts.

As part of the services, districts and the district's users also share personal information with Frontline. In these cases, the districts' privacy policies govern the use of this personal information. The districts determine what information is shared with Frontline, and districts are responsible for determining whether information is ever shared with Frontline. Frontline receives information provided by districts 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; and system usernames and passwords. In order to deliver products and services to its customers, Frontline may share this information with third party service providers for business purposes, such as third parties who provide hosting services. Districts may also direct Frontline to share this information with other third parties who provide services to the district.

Student Data: Frontline may have 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 has access to Student Data only as requested by the district and only for the purposes of performing services on the district's behalf, as directed by the district. The Student Data your educational organization shares with Frontline 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; and health-related information required for Medicaid reimbursement.

Information About You: We receive information about you when you interact with us as an individual, such as looking for a teaching position or signing up to receive a newsletter. This information includes information that you voluntarily provide about yourself, such as name, address, telephone numbers, professional and educational details, and payment information, and information that we collect through technology, as described below. We may also receive information about you from third parties, such as the results of a background check if you apply for a job with us. We do not knowingly collect, solicit, or sell information concerning anyone under the age of 16. If you are under 16, please do not use this website.

We may use, or share with our service providers, the personal information we collect for business purposes, including the following: to fulfill or meet the reason you provided the information; to provide, support, personalize, and develop our website, products, and services; to create, maintain, customize, and secure your account with us; to process your requests, transactions, and payments and prevent fraud; to respond to your inquiries, including to investigating and addressing your concerns and monitor and improve our responses; for testing, research, analysis, and product development, including to develop and improve our website, products, and services; or to respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.

Information We Collect Through Technology: We automatically collect certain types of usage information when website visitors view our website or use our services. 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 identify you faster and enhance your navigation through the site. A cookie may also convey information to us about how you use the services (e.g., the pages you view, the links you click and other actions you take on the website) and allow us to track your usage of the services over time. We may collect log file information from your browser or mobile device each time you access the services. Log file information may include 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 services. We may also collect analytics data, or use third-party analytics tools, to help us measure traffic and usage trends for the services.

We may use the data collected through cookies, log files, device identifiers, and clear gifs information to remember information so that a user will not have to re-enter it during subsequent visits; provide custom, personalized content and information; to provide and monitor the effectiveness of our services; monitor aggregate metrics such as total number of visitors, traffic, and usage on our website and our services; diagnose or fix technology problems; and help users efficiently access information after signing in. You can disable or reject cookies through your web browser but turning off cookies may adversely affect your use of Frontline's website or services. Your continued use of Frontline's website and/or services reflects your acceptance of the use of cookies, log files, device identifiers, and clear gifs.

Disclosure to Third Parties

Frontline discloses information as described in this Privacy Policy, including to service providers for business and commercial purposes. Beyond that, Frontline will disclose information to comply with a court order or other legal process served on us or assist government enforcement agencies; investigate or prevent suspected illegal activities or protect the security and integrity of Frontline Education; enforce this Privacy Policy, our Terms of Service, or other such binding agreements; take precautions against liability, investigate or defend against any third-party

claims or allegations; or exercise or protect the rights, property, or personal safety of Frontline, its employees, customers, or others.

How We Protect Your Information

Data Protection: 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. We have many unit and integration tests in place to ensure these privacy controls work as expected. These tests are run every time our codebase is updated and even one single test failing will prevent new code being shipped to production. 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 administrative, physical, and technical safeguards to secure data from unauthorized access, disclosure, and use. We will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

Incident Response: We also have a written incident response plan, to include prompt notification of the districts and educators in the event of a security or privacy breach of protected information.

Review or Deletion of District Records Maintained by Frontline: To review or update information concerning districts, schools, and their users, 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.

Data Retention: 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. 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.

Links to Other Web Sites and Services

Please remember that this privacy policy applies to the Frontline's services and websites, and not to 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.

California Privacy Rights

This section applies only to California residents who interact with Frontline as an individual including those seeking employment with Frontline. Certain individuals residing in California have specific rights regarding their Personal Information under the California Consumer Privacy Act of 2018 (CCPA). The following section describes how we collect, use and share Personal Information of California residents in operating our business, and their rights with respect to that Personal Information. Note that these rights are not absolute, and in certain cases, we may decline your requests concerning your Personal Information, as permitted by the CCPA. For purposes of this section, "Personal Information" has the meaning given in the CCPA but does not include information exempted from the scope of the CCPA.

Access to Specific Information

If you have interacted with Frontline independently, you have the right to request and receive certain information about how we have collected and used your Personal Information over the past 12 months. Such information includes: the categories of Personal Information we collected about you; the categories of sources for the Personal Information we collected about you; our business or commercial purpose for collecting and/or selling the Personal Information; the categories of third parties with whom we share the Personal Information; if we disclosed your Personal Information for a business purpose, and if so, the categories of Personal Information received by each category of third-party recipient; and if we sold your Personal Information, the categories of Personal information received by each category of third party recipient.

Deletion Request Rights

You have the right to request that we delete the Personal information we collected from you.

Non-Discrimination

You are entitled to exercise the rights described above free from discrimination in the form of legally prohibited increases in the price or decreases in the quality of our services. Accordingly, we will not discriminate against you for exercising any of your rights under the CCPA. However, the exercise of your rights may impact our websites' functionality.

Exercising Your Rights

To exercise your California privacy rights to information, access and deletion described above, please submit a verifiable consumer request to us by filling out the following form within our **Data Privacy Request Web Portal**.

Only you, or a person authorized to act on your behalf pursuant to the CCPA, may make a verifiable consumer request related to your Personal Information. In order to verify your request, we may ask you to confirm Personal Information you have provided to us.

We reserve the right to confirm your California residence to process your requests and will need to confirm your identity to process your requests to exercise your information, access or deletion rights. As part of this process, government identification may be required. Consistent with California law, you may designate an authorized agent to make a request on your behalf. In order to designate an authorized agent to make a request on your behalf, you must provide a valid power of attorney, the requester's valid government-issued identification, and the authorized agent's valid government-issued identification. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it.

Personal Information We Collect, Use and Share

We collect Personal Information when you provide it to us voluntarily, through your interaction with our websites as described above, or from third parties. We have collected the following categories of Personal Information in the past twelve (12) months: identifiers; customer / financial information and records; characteristics of protected classifications under California or federal law; commercial information; internet or other electronic network activity information; geolocation data; and professional or employment-related information. Personal Information

does not include publicly available information or deidentified or aggregated consumer information.

Use of Personal Information

We may use or disclose the Personal Information we collect as described above or for one or more of the following business purposes: auditing related to a current interaction with a consumer and concurrent transaction; detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity; debugging to identify and repair errors that impair existing intended functionality; performing services that you request, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing advertising or marketing services; undertaking internal research for technological development and demonstration; and undertaking activities to verify or maintain the quality of a service that is owned and controlled by Frontline, and to improve, upgrade, or enhance the services that are owned and controlled by Frontline.

Disclosure of Personal Information to Third Parties

In the past twelve (12) months, we have disclosed the categories of Personal Information described above for our business or commercial purposes to service providers and third parties with whom you authorize or direct us to share your information.

We have not sold Personal Information in the preceding twelve (12) months.

Privacy Rights of Job Seekers

This section applies only to California residents who interact with Frontline as a job seeker utilizing Frontline's K12JobSpot or Jobulator websites (the "Job Seeking Sites") and those seeking employment with Frontline. Certain job seekers residing in California have specific rights regarding their personal information under the California Consumer Privacy Act of 2018 (CCPA). The following section describes how we collect, use and share Personal Information of California residents in operating the business, and their rights with respect to that Personal Information. For purposes of this section, "Personal Information" has the meaning given in the CCPA but does not include information exempted from the scope of the CCPA.

Your Rights Concerning Access and Deletion

The CCPA provides consumers (California residents) with specific rights regarding their Personal Information, which are described below. Note, these rights are not absolute, and in certain cases, we may decline your request as permitted by the CCPA.

Access to Specific Information

You have the right to request and receive certain information about how we have collected and used your Personal Information over the past 12 months. Such information includes: the categories of Personal Information we collected about you; the categories of sources for the Personal Information we collected about you; our business or commercial purpose for collecting and/or selling the Personal Information; the categories of third parties with whom we share the Personal Information; if we disclosed your Personal Information for a business purpose, and if so, the categories of Personal Information received by each category of third-party recipient; and if we sold your Personal Information, the categories of Personal Information received by each category of third party recipient.

Deletion Request Rights

You have the right to request that we delete any of your Personal Information that we collected from you. As discussed above, you may also delete your information through your account.

Non-Discrimination

You are entitled to exercise the rights described above free from discrimination in the form of legally prohibited increases in the price or decreases in the quality of our services. Accordingly, we will not discriminate against you for exercising any of your rights under the CCPA. However, the exercise of your rights may impact the Job Seeking Sites' functionality and/or employers' ability to receive information about you. For example, if you delete your personal information, employers will no longer be able to access to your profile through the Job Seeking Sites.

Exercising Your Rights

To exercise your California privacy rights to information, access and deletion described above, please submit a verifiable consumer request to us by filling out the following form within our **Data Privacy Request Web Portal**.

Only you, or a person authorized to act on your behalf pursuant to the CCPA, may make a verifiable consumer request related to your personal information. In order to verify your request, we may ask you to confirm personal information you have provided to us.

We reserve the right to confirm your California residence to process your requests and will need to confirm your identity to process your requests to exercise your information, access or deletion rights. As part of this process, government identification may be required. Consistent with California law, you may designate an authorized agent to make a request on your behalf. In order to designate an authorized agent to make a request on your behalf, you must provide a valid power of attorney, the requester's valid government-issued identification, and the authorized agent's valid government-issued identification. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it.

Personal Information We Collect, Use and Share

The Job Seeking Sites collect personal information when you provide it to us or through your interaction with the Job Seeking Sites, as described above. The Job Seeking Sites have collected the following categories of personal information in the past twelve (12) months: unique identifiers, such as first name, last name, and email address, user name and password; credit card information for payment; professional / employment related information, such as education history, licenses, work experience, and extracurricular activities; commercial information, such as your communication preferences and history using the Job Seeking Sites; internet or other similar network activity, as described above; and geolocation data. Personal Information does not include publicly available information or deidentified or aggregated consumer information.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following business purposes: manage and maintain your account; provide services you request, such as disclosing your information to an employer; analyzing and enhancing our marketing communications and strategies; informing you of relevant job postings, events and announcements that may be of interest to you; operating, evaluating and improving our business and the products and services we offer; analyzing trends and statistics regarding visitors' use of the Job Seeking Sites; protecting against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure, including by identifying potential hackers and other unauthorized users; provide administrative notices or communications applicable to your use of the website; respond to your questions and comments and provide customer support;

contact you and deliver information to you that, in some cases, is targeted to your interests; enforce our website's Terms of Use; and comply with applicable legal requirements and industry standards and our policies.

Sharing Personal Information

As described above, we share your information as directed by you, such as with third party social media and with employers. We may also share your information with our service providers for a business or a commercial purpose, such as IT service providers. We have shared the following categories of personal information in the past twelve (12) months: unique identifiers; professional / employment related information; commercial information; internet or other similar network activity; and geolocation data.

In the past 12 months, we, like many companies, used services that helped deliver third party's interest-based ads to you. Our use of these services may be classified under California law as a "sale" of your Personal Information to the companies that provided the services because they collected information from our users (e.g., device data and online activity data, like browsing history) to help them serve ads more likely to interest you. We no longer do this.

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.

How to Contact Us

If you have questions about this Privacy Policy, please contact us by email, or postal mail:

- Email: security@frontlineed.com
- Address:
  1400 Atwater Drive
  Malvern, PA 19355

Updated 06/26/2020