DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

What do we mean by "Personal Information"?

For us, "Personal Information" means information or data that relates to an identified or identifiable individual. "Sensitive Personal Information" is a subset of Personal Information and is data about children, financial information, health information (including PHI as defined by the Health Insurance Portability and Accountability Act), Social Security or other national identification number, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, criminal convictions, and precise geolocation data.

We also want you to be aware certain information related to your account (for example, accounts provided by Intrado IP Communications) may be Customer Proprietary Network Information ("CPNI"). CPNI is information we obtain solely by providing telecommunications services or interconnected Voice over Internet Protocol (VoIP) services to you. It includes the type, technical arrangement, quantity, destination, location, and amount of services you purchased and related billing information. CPNI does not include your telephone number, name and address, or aggregate customer information or data not specific to you. The protection of your information is important to us, and you have a right, and we have a duty, under U.S federal law, to protect the confidentiality of your CPNI. We may use or disclose CPNI without your consent to (a) initiate, render, repair, maintain, bill, troubleshoot, and collect for our services; (b) protect our rights and property or to protect our subscribers or other carriers from the unlawful or fraudulent use of our services; (c) provide call location information required in connection with emergency services; (d) market services formerly known as adjunct-to-basic services; (e) market our services within the categories of services to which you already subscribe; and, (f) respond to a valid request from law enforcement, a court order, or other appropriate authority. Absent your consent, we will not access, use or disclose your CPNI to market categories of telecommunications or VoIP products and services that you do not already subscribe to or share your CPNI with unrelated third parties for their own use.

What type of Personal Information is collected?

We may collect data, including Personal Information, about you as you use our websites, services and interact with us. This information may include name, address, email address, IP address, phone number, login information (user name, password), marketing preferences, or payment card number. If we link other data with your Personal Information, we will treat that linked data as Personal Information. We also collect Personal Information from trusted third-party sources and engage third parties to collect Personal Information to assist us.

Please understand, in addition to collecting Personal Information, Intrado may also gather information that does not personally identify you regarding your use of the Intrado website ("Anonymous Information"). We may use the Anonymous Information we collect regarding your use of this website to measure the effectiveness of our marketing efforts, for improving the Services we offer to you, or to improve the Intrado website. Generally, you will not be aware when we collect such Anonymous Information. It may be collected in various ways, such as through traffic data or direct surveys of our customers and may entail the use of, among other things, cookies, IP addresses, or other numeric codes used to identify the computer or other device used to access the Intrado website.

How do we receive Personal Information about you?

We learn Personal Information about you when:

you give it to us directly (e.g., when you choose to contact us, or register on the Intrado website);

we collect it automatically through our products and services (e.g., your use of Intrado services);

someone else tells us Personal Information about you (e.g., our client provides us your Personal Information in order for us to perform services for them); or

when we try to understand more about you based on Personal Information you've given to us (e.g., when we use your IP address to customize language for some of our services).

Unless we receive your information through your school, or otherwise as part of our SchoolMessenger services, if you are under 13, we don't want your Personal Information, and you must not provide it to us. If you are a parent and believe your child who is under 13 has provided us with Personal Information without your express consent, please contact us to have your child's information removed. For SchoolMessenger services specific information, please see below

By providing your Personal Information, you opt-in and consent to its collection, use, disclosure, sharing, and transfer as described in this Privacy Statement.

What do we do with your Personal Information once we have it?

Intrado does NOT sell your personal information.

When you give us Personal Information, we will use it in the ways for which you've given us permission, or ways in which our clients who provided us the Personal Information instruct. Generally, we use your Personal Information to help us provide and improve our products and services for you and our clients with which you have a business relationship. We may also use the Personal Information you provide to contact you regarding additional or new services and features offered by Intrado, or important information regarding Intrado.

We may use the Personal Information to enforce our agreements with you, prevent fraud and other prohibited or illegal activities, for other legally permissible purposes and generally to ensure that we comply with applicable laws and prevent or detect use or abuse of our services.

Important Notice Regarding Unified Communications Services, Webcasting, and Virtual Event Services

Intrado processes Personal Information as part of delivering the above noted services on behalf of its customers. The customer is the data controller of the information. For these services, Intrado only collects Personal Information necessary to fulfill our contractual obligations with the customer. We may collect contact data such as name, e-mail address and company details you provide us during the registration process and during your use of the services. We may also collect product usage data, such as the date on which you viewed a webcast, the duration of your viewing and the part of the webcast you viewed.

Intrado may also use your Personal Information to create anonymous data records or aggregations of data, to perform statistical analyses and for other purposes, by omitting or removing information that makes the data personally identifiable to you.

If you have provided Personal Information to our customer, their respective privacy statement will also apply to the processing of your data. You should familiarize yourself with their statement.

How long will we retain Personal Information?

We will retain your Personal Information only as long as needed to fulfill the purposes for which it was collected or as required by law. Your information will be deleted, anonymized or pseudonymized once it is no longer needed to comply with our business requirements, legal obligations, resolve disputes, protect our assets, or enforce our agreements.

When do we share your Personal Information with others?

We will/may share your Personal Information with others:

When we have asked and received your permission to share it.

When we're required to provide it to our client from whom we received your Personal Information, or with whom you have a business relationship.

For processing or providing products and services to you, but only if those entities receiving your Personal Information are contractually obligated to handle the data in ways approved by Intrado. We may use others to help us provide our Services (e.g., maintenance, analysis, audit, payments, fraud detection, marketing and development).

To provide aggregate Personal Information to our business partners to make our products and services better, but when we do so, we will de-identify your Personal Information and try to disclose it in a way that minimizes the risk of you being re-identified.

To provide your Personal Information to business partners in case you purchase services of third parties from Intrado ("Third Party Services"). Third Party Services are not directly controlled operated or maintained by Intrado and Intrado's Privacy Statement does not apply to such Third Party Services. For any Third Party Services you purchase from Intrado, we recommend you consult the respective privacy statements of the Third Party Services providers to determine how they will handle your Personal Information.

To follow the law whenever we receive requests about you from a government entity, or related to a lawsuit. We'll notify you or our client from whom we received your Personal Information when we're asked to hand over your Personal Information in this way unless we're legally prohibited from doing so. When we receive requests like this, we'll only release your Personal Information if we have a good faith belief the law requires us to do so. Nothing in this Statement is intended to limit any legal defenses or objections you may have to a third party's request to disclose your Personal Information.

If we have a good faith belief it is reasonably necessary to protect the rights, property or safety of you, our other users, Intrado or the public.

If our organizational structure or status changes (e.g., if we undergo a restructuring, are acquired, or go bankrupt), we may pass your Personal Information to a successor or affiliate.

How do we protect your Personal Information?

We are committed to protecting your Personal Information once we have it. We implement industry standard physical, administrative and technical security measures. If, despite these efforts, we learn of a security breach involving your Personal Information, when required by law or contractual obligations, we'll notify you or our client so appropriate protective steps can be taken. Intrado is not responsible for unauthorized access to such Personal Information by hackers or others that obtain access through illegal measures in the absence of negligence on the part of Intrado.

You may have access to other sites through the Intrado websites. These sites may have different security practices and you should familiarize yourself with those practices.

How can you protect your Personal Information?

Electronic communication (e.g., email, online chat or instant messaging, etc.) you send to us may not be secure unless we advise you in advance security measures will be in place prior to you transmitting the information. For this reason, we ask you do not send Personal Information such as financial information, social security numbers or passwords to us through unsecured electronic communication. Users should also take care with how they handle and disclose their Personal Information. Please refer to the Federal Trade Commission's Web site at http://www.ftc.gov/bcp/menus/consumer/data.shtm for information about how to protect yourself against identity theft.

The Intrado website may contain hyperlinks that can take you to websites run by third parties ("Third-Party Websites"). Any hypertext or other links to Third-Party Websites from the Intrado website are provided solely as a convenience to you. If you use these links, you will leave the Intrado website. Intrado has not reviewed all of these Third-Party Websites and does not control and is not responsible for any of these websites or their content

or practices. Thus, Intrado does not endorse or make any representations about them, or any information, software, or other products or materials found there, or any results that may be obtained from using them. If you decide to access any of the Third-Party Websites linked to the Intrado website, you do this entirely at your own risk. Remember, this Privacy Statement only applies to Intrado. When you are no longer on an Intrado website, you may encounter different privacy and security practices and you should familiarize yourself with those practices each time you visit a new website.

Please be aware any information you choose to share on any publicly available portion of the Services or with third parties, including without limitation your personal page, chat messages, forum posts, blogs, resumes, job applications, business cards, or any other information you provide may be collected and used by third parties or other attendees without restriction.

How do you keep my healthcare information private?

Intrado is required by law to maintain the privacy of "protected health information." Please follow this link to Intrado's HIPAA Privacy Notice.

What about cookies and other tracking technology?

A cookie is a small file, typically of letters and numbers, downloaded onto a device when the user accesses certain websites. Cookies can make the web more useful by storing information about your preferences for a particular website or a service. Cookies in and of themselves do not personally identify users, although they do identify a user's computer.

Cookies are typically classified as either session Cookies or persistent Cookies depending on whether they expire at the end of a browser session (from when a user opens the browser window to when they exit the browser) or they can be stored for longer.

Session Cookies – allow websites to link the actions of a user during a browser session. They may be used for a variety of purposes such as remembering what a user has put in their shopping basket as they browse around a site. They could also be used for security when a user is accessing internet banking or to facilitate use of webmail. These session Cookies expire after a browser session, so would not be stored longer term. For this reason, session Cookies may sometimes be considered less privacy intrusive than persistent Cookies.

Persistent Cookies – are stored on a user's device in between browser sessions which allows the preferences or actions of the user across a site (or in some cases across different websites) to be remembered. Persistent Cookies may be used for a variety of purposes including remembering users' preferences and choices when using a site or to target advertising.

Intrado uses cookies or other similar tracking technologies to provide you with better Services.

Most browsers are initially set to accept Cookies. You may configure your browser to accept all Cookies, reject all Cookies, or notify you when a Cookie is set. You can manage your own Cookies preferences by using your browser settings: each browser is different, so check the "Help" menu of your browser to learn how to change your Cookie preferences or delete them. If you prefer, you can set your browser to refuse Cookies. You block Cookies by activating the setting on your browser which allows you to refuse the setting of all or some Cookies.

Please note you may browse some Intrado websites without accepting Cookies from Intrado; however, you may not be able to take full advantage of the functionality of the website or the Services if you do so. Other Services, particularly those which require a login and password, require Cookies and cannot be used when you have disabled Cookies in your browser. For more general information, you can visit www.allaboutcookies.org.

How do you handle my "Do Not Track" browser settings?

Intrado does not track the non-Intrado website activity of any internet user with Do Not Track browser settings engaged.

Does Intrado use any other tracking technology?

Intrado employs a software technology called transparent images to help us better manage content on our site by informing us what content is effective. We use extremely small, transparent images with a unique identifier, similar in function to cookies, used to track the online movements of Web users. The main difference between the two is transparent images are invisible on the page and are very small, about the size of the period at the end of this sentence. In some instances, transparent images are tied to users' personally identifiable information. In particular, we use transparent images in our HTML-based e-mails to let us know which e-mails have been opened by the recipients. This allows us to gauge the effectiveness of certain communications. Users may opt out of these e-mails by replying to the unsubscribe link at the end of the e-mail message.

How does Intrado ensure compliance with legal obligations?

In connection with the Services, and if applicable, you and Intrado shall at all times ensure compliance with any privacy and data protection laws including those in the United States (including but not limited to the Gramm-Leach-Bliley Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, California Consumer Privacy Act and the Fair Credit Reporting Act), in the United Kingdom (including but not limited to the Data Protection Act), in the European Union (including but not limited to relevant EU member state legislation and the General Data Protection Regulation), in the Asia-Pacific Economic Cooperation (including but not limited to Australia's Privacy Act along with the Australian Privacy Principles, Singapore's Personal Data Protection Act, Japan's Act on the Protection of Personal Information and Hong Kong's Personal Data (Privacy) Ordinance) and anywhere around the world.

We're a global organization and our information systems are in several countries around the world. We also use service providers whose information systems may also be in various countries. This means your Personal Information might end up in one of those information systems in another country, and that country may have a different level of data protection regulation than yours. The whole or any part of your Personal Information in connection to the Services may be processed by Intrado, its affiliates and subcontractors in the United States, United Kingdom, the European Union, Philippines, India, Canada, Mexico and the rest of the world, and may be transferred outside the country in which you provided the Personal Information. By giving us Personal Information, Intrado may conduct such transfers of your Personal Information. No matter what country your Personal Information is in, we comply with applicable law and will also abide by the commitments we make in this Privacy Statement

Does Intrado participate in EU-U.S., UK-U.S. and Swiss-U.S. Privacy Shield?

Intrado entities which include Intrado Enterprise Collaborations, Inc., Intrado IP Communications, Inc., Intrado LLC, Intrado Digital Media, LLC, Intrado Communications Holdings LLC, INXPO, Zferral, Inc. dba Ambassador and Intrado Interactive Services Corporation ("Intrado Privacy Shield Entities") comply with the EU-U.S. Privacy Shield Framework, UK-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information transferred from the European Union, the United Kingdom, and Switzerland, respectively, to the United States. Intrado Privacy Shield Entities have certified to the Department of Commerce they adhere to the Privacy Shield Principles. If there is any conflict between the terms in this privacy statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certifications, please visit https://www.privacyshield.gov/. The Intrado Privacy Shield Entities recognize the Federal Trade Commission has jurisdiction over their compliance with the Privacy Shield.

Pursuant to the Privacy Shield Frameworks, EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Privacy Shield, should direct their query to privacy@intrado.com. If requested to remove data, we will respond within a reasonable timeframe.

We will provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to privacy@intrado.com.

Intrado's accountability for personal data that an Intrado Privacy Shield Entity receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, the Intrado Privacy Shield Entities remain responsible and liable under the Privacy Shield Principles if third-party agents it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless the Intrado Privacy Shield Entities prove they are not responsible for the event giving rise to the damage.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, Intrado Privacy Shield Entities commit to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union, UK, and Swiss individuals with Privacy Shield inquiries or complaints should first contact Intrado by email at privacy@intrado.com or by mail at the address below.

Intrado has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit http://www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

How do you handle my Personal Information as part of the SchoolMessenger Solution products and services?

Except as we describe in this section, we handle it as described above. This section is limited to Intrado's SchoolMessenger Solution products and services.

In general, we do not knowingly collect Personal Information directly from students, including children under 13, but only as shared with us by our customer agency/institution. Exceptions are a student username, password and related account login credential information that we collect directly from the student if necessary when they login to our services as authorized by their school. By default, students cannot create an account – to enable our direct collection of their Personal Information – without the school's consent. When we do collect student Personal Information directly from students, including children under the age of 13, we do so only on behalf of and under the direct control of our client, and the client is responsible for obtaining any necessary prior parental consents. Should we learn that we collected Personal Information from a child under 13 and our client does not provide proof of consent within a reasonable time, we will delete all such Personal Information. We do not enable or encourage students to make their Personal Information publicly available.

When you use our school and other mobile applications, you may also be prompted to grant the app access to certain information and functions on your device, including your device ID, geolocation information, and calendar. We do not access this information, which remains on your device. This information is necessary for your device to enable the app to remain updated with the latest school information such as receiving push notifications, importing calendar events, and identifying nearby schools.

We do not sell, trade, lease or loan the Personal Information we collect or maintain to any third party for any reason, including that we do not sell or otherwise share student Personal Information with direct marketers, advertisers, or data brokers.

We do not share student Personal Information with third parties, though a few of our service providers may have

limited access to such information within our data systems in the course of their providing us with data analytics, software programming and related services to support our service delivery, evaluation or improvement. In some instances, we store student Personal Information with a third party data hosting provider, though student Personal Information is secured through access controls and electronic protection methods meant to prevent unauthorized access. We have agreements in place with all third parties with access to student Personal Information to ensure they only use the information for purposes necessary to deliver the authorized service to us and to ensure they maintain the confidentiality and security of the information.

If you are the administrator of an educational agency/institution customer account and have any questions about this statement or if you believe we are not handling your information in accordance with our privacy statement, please contact us at the applicable address above.

If you are otherwise a user of one of our school services, we encourage you to first contact your educational agency/institution with any questions or concerns regarding this privacy statement or our handling of Personal Information.

How do you handle my Personal Information as part of GlobeNewswire's Media Contacts Database products and services?

Certain of our GlobeNewswire services provide detailed profiles for media contacts and news outlets to public relations, media and marketing professionals, such as yourself. If you are receiving these types of emails from GlobeNewswire, it is because your professional contact information is publicly available and we believe there is a legitimate interest and/or implied consent for you to be part of our media contacts database, which includes data in the public relations industry compiled by our in-house research team. If you do not wish to be part of our media contacts database, you may unsubscribe at any time by clicking unsubscribe at the bottom of an email you have received from us. We may use your Personal Information for purposes related to data analytics with our third party partners. By fully unsubscribing your Personal Information will not be used this way.

China Users

If you use our services in the People's Republic of China, your personal data is collected, processed and/or stored by Intrado, its affiliates and their third party suppliers in the People's Republic of China, the United States of America and other locations in the rest of the world. By using the services in the People's Republic of China, you hereby consent that (a) your personal data may be transferred outside of the People's Republic of China to the locations noted herein and (b) Intrado and its affiliates and their third party suppliers may collect, process and or/store your personal data in order to provision the services.

What choices do you have regarding your Personal Information?

We are aware you have several rights in respect to how we process your Personal Information, which include but are not limited to, a right to access your Personal Information, be forgotten, restrict and/or object to processing in some circumstances and request your Personal Information be transferred to you or your nominated third party.

You may choose not to have your information disclosed to a third party (unless Intrado is legally required to share it). You may also choose to not have your information used for a purpose materially different than the purpose for which it was originally collected or subsequently authorized by you.

We will take reasonable steps to give you the opportunity to correct inaccuracies in the Personal Information we retain concerning you and delete Personal Information concerning you upon your request, unless the burden or expense of providing access would be disproportionate to the risks to your privacy or where the rights of persons other than you would be violated. We may deny a request to delete your data if we have legal obligations to retain it. Any such data will be subject to our standard retention guidelines.

You are entitled to know whether we hold personal data about you and, if we do, to have access to that personal data and require it to be corrected if it is inaccurate. In some circumstances, you may have the right to oppose the use or disclosure of your data or have your data deleted. You can do this by contacting us as directed in the

"Contact Us" section below.

To correct inaccuracies in your Personal Information, limit purpose of use and disclosure, delete your Personal Information, or for any other requests or questions, please contact us as directed in the "Contact Us" section below. Once we have verified your identity, we will complete the request from you or an authorized agent you have designated. We will make all efforts to verify your identity using information we already have but may need to request additional data if we are unable to make the verification on this data alone. If you designate an agent to make requests for you, we reserve the right to ask for proof of the agency.

Intrado will not discriminate against any individual for exercising their privacy rights outlined above. This includes, but is not limited to; denying goods or services, change in pricing or lower quality goods or services.

What if we change this Privacy Statement?

We may need to change this Statement and our notices. Unless otherwise required, the updates will be posted online. If the changes are substantive, unless otherwise required, we will announce the update through Intrado's websites. Unless further steps are necessary related to the changes, your continued use of the product or service after the effective date of such changes constitutes your acceptance of such changes. To make your review more convenient, we will post an effective date at the top of the page.

How to Contact Us?

If you want to make a correction to your Personal Information, or you have any questions about our privacy statement, please contact the privacy team by emailing privacy@intrado.com, contacting us toll-free at 1-855-760-5025, outside of the U.S. +1-402-702-2390 or by mail, we can be contacted at:

US

Janette Nelson, Vice President & Deputy General Counsel

Intrado

Legal Department

11808 Miracle Hills Drive

Omaha, NE 68154

INTERNATIONAL

Steven T. Taylor, Senior Director & Privacy Counsel

Intrado

Legal Department

175 Bloor Street East

South Tower, Suite 900

Toronto, Ontario M4W 3R8

Canada

EUROPEAN UNION – GDPR

Intrado

Legal Department

4 Rue Charras

Paris 75009

France