

Linewize Monitor

Onboarding Guide

Helping school districts detect
online risks before they
become real-life incidents.

Contents

Digital Monitoring	3
How it works	4
Our Moderation Team	5
Getting Started	5
Using Monitor	6
Organizations	6
Safeguarding Contacts	6
Alerting Profiles in Monitor	7
Dashboard	7
Events in Monitor	7
Alert Levels & Phone Calls	8
Risk Categories	8
Best Practices	8
Appendix A: Monitor Glossary	11
Appendix B: Linewize Staff and Additional Support	13

Digital Monitoring

As you know students' safety is our #1 priority, and we want to make sure your district is prepared and your students are protected. Monitor will help you identify problematic online behaviors so that vulnerable students can be helped faster and more holistically. Their digital behavior will provide a comprehensive report of early warning detections of risks or incidents that may otherwise go unnoticed.

- Gun violence, mental and behavioral health issues, bullying and suicide are at an all time high for our youth
- There are often early indicators and signs of these potential issues within the digital data that happens on school devices
- Monitor gives you real-time alerts and detailed data to assess the specific urgency in which your district needs to prioritize student wellbeing

Signs of distress are not always seen. Monitor gives you the ability to look under the surface to identify risk and respond when and where there is a real need.

Offline risks you can see



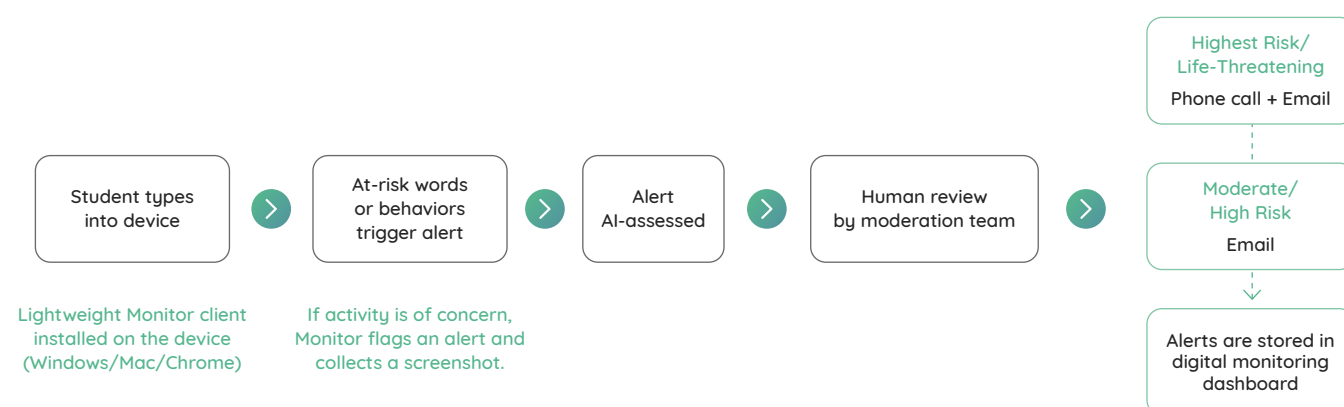
Changes in behavior. Injuries/bruises, tip-offs from peers, absenteeism.

Digital risks you can't see



Online bullying or conversations about drugs/extremism/being harmed, hidden bruises/injuries, unspoken negative feelings and thoughts.

How it works



- Student online activity indicates risk.
- AI (artificial intelligence) and NLP (Natural Language Processing) capture and perform a preliminary assessment of risk across 9 categories, which is reviewed by the Moderation Team. Our Moderation Team works 24-hours so that the flagged content is reviewed in real time.
- There are 3 ways that you can see the flagged content.
 - Events page in Monitor
 - Email Alert
 - Phone call
- All flagged content that is reviewed by our Moderation Team can be viewed in the Events section in the Monitor Portal.
 - Integrates AI with human decision-making (Moderation Team), which reduces workloads, false-positives, and improves accuracy.
- For activities rated Mod/High risk without the threat of imminent harm to self or others, your Safeguarding Contacts will receive an email alert from noreply-monitor@linewize.com.

If the risk is assessed to be an imminent risk to serious bodily harm or potential loss of life, your Safeguarding Contacts will receive a phone call from **1.858.666.6910**.

When you receive a phone call, our Moderator will identify themselves as calling from Linewize. They will inform you that we have identified a high risk event and more detailed information has been sent in an email. Please note, our Moderators have limited access to student information in order to protect the privacy of your students.

Note: you can make adjustments to which emails you receive.

Our Moderation Team

Our Moderation Team is a highly skilled team that works 24 hours a day so that moderate to high risk events are reviewed in real time. Our Moderators work as a team prioritizing the high priority queues.

Our Moderators undergo rigorous training and ongoing professional development and supervision. Their training includes working in a test environment as they build their skills, shadowing experienced Moderators, and then working side-by-side with a Team Lead until the Team Lead is confident in their abilities.



Getting Started

The below outline highlights our Monitor onboarding process.

1

CSM Intro & Next Steps Meeting

During this call, your CSM will introduce themselves, discuss current success criteria and suggest updated success criteria, review the Linewize Learning Resources with you and your team, and coordinate scheduling a series of essential meetings to ensure a successful deployment (meetings listed below).

2

Monitor Training Meeting

During this meeting, you will work with our Engagement team to explore your settings and how you may adjust them to meet your unique goals, discuss contact types and their roles within the platform, and share best practices for training other users with Monitor. By the end of the meeting, you will be able to confidently adjust your Monitor settings if needed before your deployment and go live.

3

Final Deployment Meeting

During this meeting, your CSM and Deployment Engineer will review the deployment checklist with you, confirming all items on the list have been completed and signifying the completion of the deployment process. After this meeting, your CSM will share additional information on contacting support and a reminder of upcoming meetings.

You will be provided with access to our Monitor learning resources. It is highly recommended that your Monitor users review these materials and watch the on-demand video before they start receiving alerts.

Being adequately prepared to receive and respond to emails and phone calls is a key determinant of the successful implementation and application of this technology within your school district.

Using Monitor

Go to <https://monitor.linewize.net/> to log into Monitor.

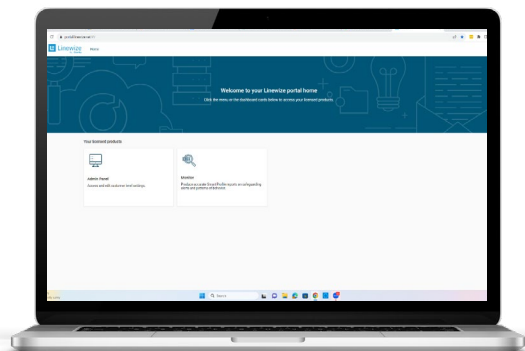
To learn how to get the most out of your Monitor application, visit:

- [Monitor Help Center](#)
- [Linewize Learning Resources](#)

Using Monitor Organizations

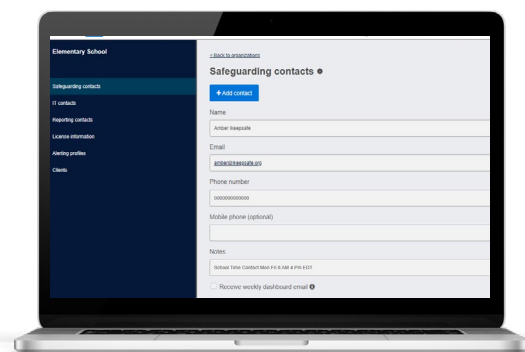
All participating schools in your district will be visible in the Organizations tab. Organizations are also referred to as Schools or Tenants.

If you click on the **Edit** button, you will be able to see your Safeguarding Contacts.



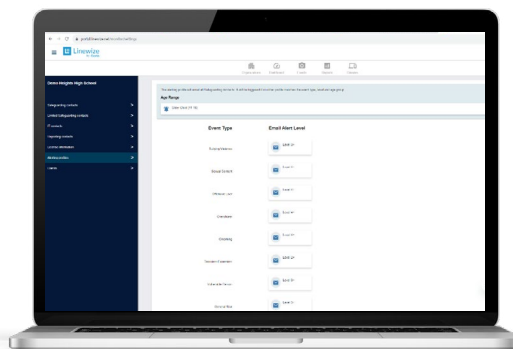
Using Monitor Safeguarding Contacts

- **Safeguarding Contacts:** Contacts that will be notified when flagged activity occurs based on alerting preferences set by your school.
- **Limited Safeguarding Contacts:** Will only receive alerts for groups that they are assigned.
- **Reporting Contacts:** Contacts that can only view high-level, summary information about Monitor. Does not have access to individual event details.
- **IT Contacts:** Contacts that view and manage your school's installed devices.



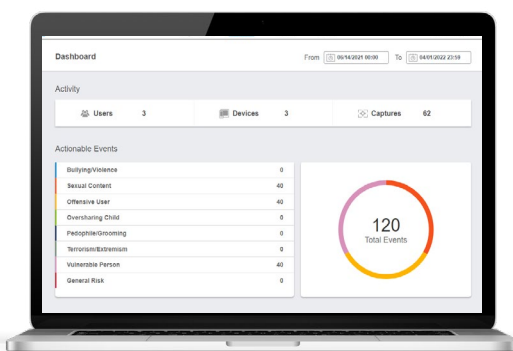
Using Monitor Alerting Profiles in Monitor

This is an example of what your Alerting Profiles will look like. The level determines which emails you will receive. If you lower the Email Alert Level, you will receive more emails. Conversely, if you increase the Email Alert Level, you will receive less emails.



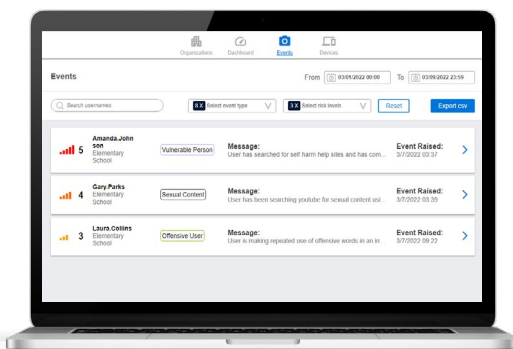
Using Monitor Dashboard

Dashboard provides a visual overview of the number of total events and number of events in each risk category. You can choose a date range to view these events.



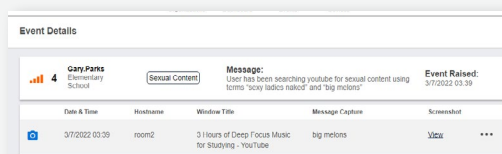
Using Monitor Events in Monitor

On the Events page, you can see all the events that Monitor has detected. Events may also be referred to as instances or flagged content. You have various options for sorting the events, depending on your needs. You can even export the events in a csv file. Monitor saves the events for 15 months.



Event Details

- Alert level
- Risk Category
- Student Name
- Organization (school)
- Message from the Moderator (if it is a Moderate to High Risk Event)
- Date and Time Sent from Moderator
- Screenshot (if available)



Alert Levels and Phone Calls

- Each event is rated 1 to 5, with 1 being the lowest and 5 being the most severe.
- Our AI technology sends each event to the Moderation Team for review.
- Phone calls are made by our Moderation Team when there is an imminent risk of serious harm or loss of life for the student or others.

What happens after the Moderation Team reviews the flagged content?

If the flagged content falls into one of the Risk Categories with a severity level between one and five, the Moderation team raises an event alert in Monitor for you to review and act. The event alert shows against a risk category with a risk level.

If the combination of the two requires it, as per the alert procedure, the Moderation team also emails the safeguarding and/or limited safeguarding contacts and, in some cases, phones the assigned contact(s) for the school.

Why would the moderation team make a phone call?

If there is a risk of imminent harm to a student or another person that could result in serious injury or loss of life, the Moderation team will alert the assigned contact(s) with a phone call.

Please note, the Moderators making the phone calls will not have access to the student's name or other personal information. This is a safeguarding measure to protect the privacy of your students.



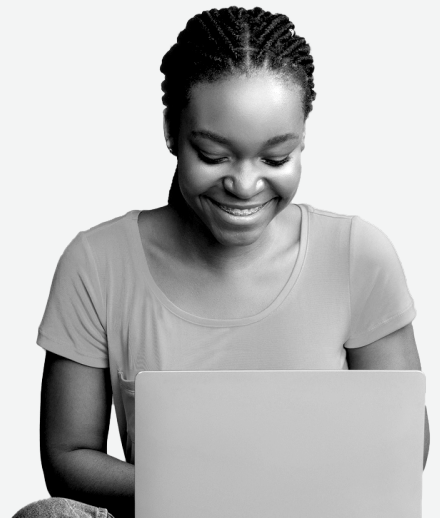
Moderators making the phone calls will **not have access** to the student's name or other personal information.”

Risk Categories

Profile	Description
Bullying	A person who singles out individuals for a campaign of intimidation, abuse, harassment, and/or exclusion and may encourage others to join in. Someone who may post material intended to shame and humiliate their target and regularly engages in personal abuse against others.
Violence	<p>A person who:</p> <ul style="list-style-type: none"> • Communicates threats of bodily injury or death to a person • Engages in physical force intending to hurt or damage a person or property • Physically intimidates, harasses or is violent towards others • Performs detailed research or shows interest in weapons or guns • Or is the target of threats of physical injury or death.
Sexual Content (Turned off during SSA but available for full deployment)	A person who makes frequent sexual overtures to others or engages in cyber-sex or talk of a highly sexual nature.
Offensive User	A person who engages in high use of profanity, without personally abusing others in a bullying manner. One who may introduce subjects or images that are highly distressing to others.
Oversharer	A person who regularly attempts to share personal information that would make them contactable online or offline or would result in a serious personal data breach.
Paedophilia/ Grooming	<p>A person who is suspected to be over the age of 18 who has contact with someone for sexual purposes who is suspected to be under the age of 18. A person who may establish trust with the child by appearing sympathetic to their problems, is on their side, and may encourage the child to share details about their life or information that will make them contactable online or offline.</p> <p>A person may establish the child's sexual experience, desensitize the child to sexual discussion, normalize it and encourage the child to participate in it. Someone who may send or request nude photos or webcam sessions with the child and who may ultimately attempt an offline meeting.</p>
Terrorism/ Extremism	<p>A person who makes direct threats to undertake acts of terrorism including bombing, biological attack, kidnap, and execution against a high-profile target or general public.</p> <p>OR</p> <p>A person who promotes terrorist activity carried out by others as rational, morally just, or a duty. One who encourages others to carry out unofficial or unauthorized acts of violence or intimidation against others in the pursuit of their political or religious aims. A person who encourages demonization of those outside their ideological sphere, often with the use of political or religious propaganda.</p>
Vulnerable Person	A person who makes credible threats of suicide or self-harm or engages in suicidal talk. Someone who appears to be at current risk of sexual or physical abuse offline or is giving indications of suffering from an untreated eating disorder, other mental illness, or being severely distressed.
General Risk	This is used for situations where our Moderation team has spotted something unusual or concerning, which they feel the school should be alerted to and doesn't fit clearly inside any of the other category descriptions.

Best Practices

- Confirm school's/district's response protocol and how Safeguarding/Limited Safeguarding contacts will respond to emails/calls
- Save alert phone number **(1.858.666.6910)**
- Save alert email sender (noreply-monitor@linewize.com)
- Data collected starts on Monday at midnight - in order to view Monday data for the current week, set date range back to previous week



Appendix A:

Monitor Glossary

Admin Panel: Section of Monitor where Global Admin can access and edit customer level settings such as Directory Integration and creation of Groups. (See also Global Admin)

Alerts: Notification of an event in Monitor through email and/or a phone call, depending on the risk level of the event. All events can also be seen on the Events page in Monitor.

Alerting Profile: Alerting profiles are customized profiles for reporting on Groups. Each school/organization has a default Alerting Profile set for your Safeguarding Contacts. The Alerting Profile sets the criteria for the email alerts your Safeguarding Contacts will receive. You can integrate your student directory and use that directory to create Linewize Groups. You can assign each Linewize Group a customized Alerting Profile and designated Limited Safeguarding Contacts. (See also Groups)

Client: On Windows or Mac devices, the software that enables Monitor to run on student devices. The Unique School Organization ID's are then utilized in the deployment of the Monitor client to Windows or Mac devices. (See also extension)

Contacts: Monitor uses Contacts to allow the people who support your users and your school the correct level of access to data about your users, devices, reports or synced data.

Dashboard: In Monitor, your dashboard provides an overview with the number of events in each category over a specific time period.

Events: Can also be referred to as instances and/or flagged content. Events are what the AI system analyzes. These events can be seen in Monitor in the Events Section.

Extension: On Chromebooks, the software that enables Monitor to run on student devices. The Unique School Organization ID's are then utilized in the deployment of the Monitor client to Chromebooks. (See also client)

Global Admin: This is the person at your district (in most cases, your head of Technology) with access to the Admin Panel. This person can integrate the directory to create Linewize Groups, view tenant, account and license information, add Cloud Scan integration and create Monitor scheduling.

Linewize Groups: You have the ability to integrate your school directory and create subgroups within each organization. Once you have created these groups, you can create unique Alerting Profiles for each group and Limited Safeguarding Contacts to receive only the alerts from a specified Group.

IT Contacts: This type of contact has the most restricted access within the Monitor portal. They can:

- Manage IT contacts
- View alerting profiles
- View and manage installed devices. (See also Contacts)

Limited Safeguarding Contacts: This contact has more limited access than the Safeguarding contact. They:

- Receive email alerts and phone calls for an alerting profile they have been added to
- Have limited access to the portal to view these alerts, but with no access to the other areas within the portal
- View events page filtered for students in their Alerting Profile.

Appendix A: Monitor Glossary cont.

Moderation Team: A group of highly trained individuals who review all Medium to High events. A member of the Moderation team will review the event and make a determination of level and if the risk level of the event warrants an email and/or a phone call. **In an effort to protect student privacy, Moderators do not have access to names or other identifying information.**

Organizations: Each school in your district that is using Monitor (also called School or Tenant).

Risk Levels: In Monitor, each event is given a Risk Level on a 1 through 5 scale, with 1 being the lowest risk and 5 being the highest.

Risk Categories: Monitor screens for 9 risk categories. These categories are:

- Bullying
- Violence
- Offensive User
- Sexual Content
- Vulnerable Person
- Oversharer
- Grooming
- Terrorism/Extremism
- General Risk

Safeguarding Contacts: This contact type has full access to the portal. This means that they can:

- Receive email alerts
- Review events in the Monitor portal
- View and manage installed devices
- Manage Safeguarding, Limited Safeguarding, IT, and Reporting Contacts (see also Contacts).

Reporting Contacts: This contact type has limited access to the Monitor portal. They can:

- Manage Reporting Contacts
- Receive weekly emails
- Access the Monitor dashboard
- View alerting profiles.

Tenants Report: This feature is only available when your district has more than one organization. The Tenants report allows you to compare trends across organizations within your district.

Appendix B: Linewize Staff and Additional Support

Monitor Support: For issues related to your Monitor deployment or configuration, syncing, or any technical issues: Click on **"Contact Support"** at the top right of your Monitor screen to submit a support ticket, or you can email **help@linewize.com** or call **844-723-3932** for assistance.

Deployment Engineer: The deployment engineer will meet with you to set up Monitor for your district. For questions related to deployment, directory integration, and syncing, reach out to the deployment engineers.

Sale Representative: Your Sales Representative will guide you through the purchase process. Once you make the decision to purchase Monitor, your Sales Representative will set up a district wide deployment planning call where Sales will introduce you to your Customer Success Manager.

Customer Success Manager/CSM: All of our customers have a CSM. Your CSM will be your primary point of contact throughout your time with Linewize and will provide regular check-ins with you and your team, serve as an escalation point for any issues or challenges, and keep you apprised of new product features!

Customer Engagement Consultant: During the Monitor discussion meeting, we will discuss best practices for using Monitor in your district and plan the training of your contacts, who will be receiving alerts.

You can reach the Customer Engagement Team at **engagement@linewize.com**.



Linewize is the leading provider of digital safeguarding solutions in the U.S. For more information, visit our website or get in touch with our team of experts.

Web: www.linewize.com

Tel: 844 723 3932

Email: sales@linewize.com

Qoria

Linewize is part of Qoria, a global technology company, dedicated to keeping children safe and well in their digital lives. We harness the power of connection to close the gaps that children fall through, and to seamlessly support them on all sides - at school, at home and everywhere in between.

Find out more
www.qoria.com