



# Debunking 9 Student Privacy Concerns Around Online Monitoring Systems

Learn the truth about the most widely  
circulated myths around student  
online monitoring technology.

# Introduction

**Many parents are concerned about how schools use student data and how monitoring tools might inhibit the learning experience.**

With the growth of remote learning and 1:1 initiatives in schools throughout the country, now is a better time than ever to discuss the privacy of students and the myths that perpetuate anti-monitoring views.



As a leader in online student online monitoring technology, Linewize's goal is to continue contributing to privacy and safety-related conversations in meaningful ways.

After thorough research, we've discovered a few myths about privacy concerns related to student monitoring. In this article, we'll debunk some of the most commonly circulated misconceptions.

"Using monitoring software alone doesn't amount to much more than surveillance," cautions Teodora Pavkovic, the lead digital wellness and online safety expert at Linewize.

"When you add conversation to that—and lots of it—you create that vital dialogue around digital citizenship, healthy online habits, and socialemotional well-being."

## 1) Monitoring Tools Substitute Mental Health Counselor Support

**No monitoring tool—no matter how robust the technology—can replace or replicate the need for a real, on-site mental health support system.**

Every school should have the resources in place to provide students with a comprehensive self-harm prevention strategy and qualified counselors to assist with any other issues that may arise.

The right monitoring technology solutions provide support and evidence to professional guidance counselors and school liaison officers. It enables mental health staff to target risks with accurate precision and plan interventions with greater efficiency. And ultimately, it optimizes staff time and resources.

## 2) Monitoring Technology Exists Because of Remote Learning

**Contrary to what many believe, schools have been using monitoring tools for decades.**

Since the Internet became a mainstay in the educational system, the government has implemented many federal regulations regarding privacy protection and Internet usage on school premises.

These include:

- 1. Children's Internet Protection Act (CIPA):** Congress enacted CIPA in 2000 to address concerns regarding children's access to obscene or harmful content over the Internet.
- 2. Children's Online Privacy Protection Rule ("COPPA"):** Enacted in 1988, COPPA protects the privacy of children under the age of 13 by requiring parental consent for the collection or use of any personal information of the users.
- 3. Family Educational Rights and Privacy Act (FERPA):** FERPA was enacted to protect the privacy of student education records.

These federal laws require schools to put efficient safeguards in place to protect students and preserve the learning environment. Therefore, since these laws were passed, it has been mandatory for schools to "filter" and/or "monitor" student online activity.

With the proliferation of remote learning and the acceleration of technology-use in the classroom, organizations like Linewize have developed tools that both ensure compliance and address growing safety concerns in schools.

Lastly, the need for monitoring, in part, comes from the fact that schools are the main 'supplier' of technology for children. Because schools require children to use technology in the classroom, they therefore also need to put in place safeguards that ensure children are safe while using that technology.

If children's learning were less tech-saturated, there would also be less of a need for safeguarding.

## 3) Monitoring Technology is Unnecessary

**Monitoring technology has proven to be a positive and necessary tool for schools across the country.**

In 2021, data collected from Linewize Monitor found that:

- Every 5 minutes we spotted a child at serious risk. (71% increase on the previous year.)
- Every hour we found a child facing a very serious risk to their health or life.
- Every hour we found a child involved in a life-threatening cyberbullying or violence incident.
- Every 12 minutes we found a child involved in a serious sexual incident.

## 4) Collected Data is Never Deleted

Many companies have come under scrutiny for their invasive data collection policies. Understandably, it's scary to think that any app or service you use collects your data indefinitely.

**This isn't the case with online monitoring software, which needs to adhere to the aforementioned federal laws regarding the protection of student data.**

## 5) Every Sensitive Subject is Flagged - Even if it Isn't a Threat

**EdTech solutions only flag instances considered risky by a combination of advanced AI-aided technology and human moderators.**

Many monitoring tools are sophisticated enough to understand the difference between creative expression and harmful online activity.

For example, if a middle school student is researching the negative effects of drugs for a term paper, that student would not be flagged. Issues that are prematurely flagged for non-risky behavior are referred to as "false positives."



## 6) Teachers Analyze Student Monitoring Data Often

**The notion that teachers use monitoring tools to see what their students is doing outside of class hours is unprecedented.**

According to a study published by the National Center for Education Statistics, many teachers feel overworked. The right technology should reduce the amount of stress and administrative workload teachers handle.

There's a difference between student monitoring technology and classroom management technology. Classroom management software, like Linewize's Classwize, allows teachers to conduct and manage technology-aided classroom sessions.

Monitoring, on the other hand, keeps a watchful eye on potential risks without classroom interference.



With other solutions we've had to be on top of the alerts so we don't miss anything. That means going through tons of false positives. Linewize Monitor has allowed us to step back a little."

**Lenny Libitz, Chief Technology Officer  
South Bound School District, NJ**

## 7) Schools Weaponize Data to Control Student Behavior

**While no one can speak for every school, it goes without saying that no faculty member should weaponize data in an effort to control student behavior.**

Unfortunately, rumors of this behavior have led many people to consider this type of dictation as the rule and not the exception.

Schools should work with their community to relay information about how their monitoring technologies works, what it's used for, what data is collected, and how data is stored. Building transparency around monitoring tools can cultivate a community of shared values and goals.



The need for transparency should be top-of-mind for every school that decides to implement monitoring technologies,” **says Teodora Pavkovic, the lead digital wellness and online safety expert at Linewize.**

“We have heard of instances where parents and students found out months after-the-fact that school-issued devices were being monitored, and this understandably caused a severe breakdown of trust in school leadership.

A huge part of implementing this type of technology successfully involves making sure that both parents and students understand what is going on, what the technology entails and what it doesn't, and that they feel their opinions and feelings are being valued.”

### Informing inappropriate behavior

Any school staff member, student, or parent that learns about a situation where student data is leveraged against a student without merit - or where monitoring technology is communicated using fear-mongering language (i.e., “we can see everything you're doing”) - should be reported immediately.

## 8) Monitoring Tools Can Spy on Students

There is a widely circulated misconception that monitoring tools “spy” on students, with some myths claiming monitoring tech has the ability to activate a student’s webcam.

**This couldn’t be further from the truth.**

Even when students are in remote school classes with cameras turned on, online student monitoring technology cannot access the device’s camera or microphone.

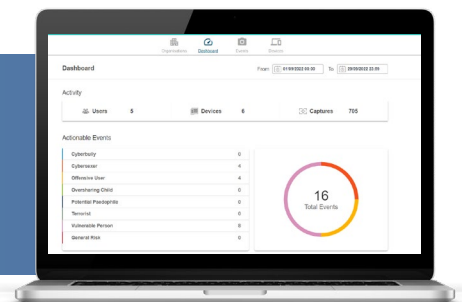
Think of tools like Linewize Monitor akin to a motion sensor light; it’s always working silently in the background but “activates” when it detects a potential risk on a schoolissued device. It then captures a screenshot of the potential risk for additional assessment from artificial intelligence technology and highly-trained Linewize human moderators.

## 9) Monitoring Technology is Primarily Used to Identify Students at Risk of Self-harm

Online monitoring technology has been closely associated with the term “self-harm prevention.” **However, there are many use cases for monitoring technology; the ability to identify potential self-harm risks amongst the student population is just one of them.**

Monitoring tools like Linewize Monitor detect risks across seven key categories, including violence, bullying, suicide, drugs, abuse, extremism, and oversharing.

Learn more about Linewize Monitor  
**Book a free demo**





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](http://www.linewize.com)

**Tel:** 844 723 3932

**Email:** [sales@linewize.com](mailto:sales@linewize.com)



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](http://www.qoria.com)