GoGuardian

Protecting Students and Their Privacy

A 4-Step TACT-ical Approach

Supporting student safety and privacy is possible with transparency, access, communication, and teamwork.

Even before the COVID-19 pandemic sent schools online, the growing presence of technology in classrooms has moved student safety and privacy topics to the forefront of conversations in districts across the country. Access to devices and the internet has created countless opportunities for enhancing learning, creating efficiencies for educators, and multiplying resources available to school communities — but the internet is a vast and varied place. The need for online safety is especially clear when considering the U.S. Surgeon General's advisory highlighting the urgency of the nation's youth mental health crisis.

How do schools leverage these valuable digital resources while protecting their school community?

At the heart of this matter are two complex issues that, at times, seem in opposition — student safety and privacy. Parents, caregivers, educators, and community members, however, want schools to protect both students' safety and their privacy. With this in mind, it's more important than ever for schools to have a thoughtful and comprehensive approach to implementing student safety technologies.

Internet Access and Student Mental Health

Today's students spend a lot of time working, communicating, and exploring online. Remote learning during the pandemic reaffirmed the vital role technology has in the future of education. A new survey conducted by survey research company Morning Consult polled a nationally representative group of nearly 2,500 K-12 parents, teachers, and administrators and found:

- **93% of parents and 98% of teachers and administrators agree the internet is a useful learning tool** schools should use as part of their learning process.

> Additional details and visual representations of key survey findings from Morning Consult can be found here.

The same study found that **74% of K-8 and 68% of 9-12 parents are concerned about students accessing explicit or harmful content** while using a school-issued device — this concern increases to **more than 80% for teachers and administrators.**

Here's what else they discovered:

- **Concern for student safety is high:** More than 83% of K-12 parents and caregivers, educators, and administrators feel a high level of concern for student mental health and violence in schools.
- **Unrestricted access can be detrimental or harmful:** Over three in four respondents agree unrestricted access to the internet on school-issued devices can be detrimental to student mental health.
- **The internet plays a role in influencing self-harm or violence:** More than 72% of respondents agreed the internet plays a strong role in influencing students to harm themselves or others.

These concerns are validated in other data; internet searches related to self-harm and suicide are common amongst youths, particularly those with suicidal thoughts and behavior.[1] Additionally, the COVID-19 pandemic underscored the critical role schools play in supporting students' mental health needs. Prior to the pandemic, **70-80% of students who received mental health services received them through their schools.**[2]

With how much time students spend online, schools across the country are looking to deploy technologies that can help protect all students from dangerous and harmful content while also urgently escalating instances where a student may be at risk of suicide or self-harm.

Teddy Hartman, Head of Privacy at GoGuardian, suggests thinking about online safety the same way we think about safety at school. Parents expect schools to keep children safe while in a classroom or on a field trip — that they will be in the company of vetted adults, aboard school buses that have passed inspection, etc. Hartman asks, "If we extend that thinking to the digital learning environment, what sort of expectations can parents have for the school's online safety guardrails?"

Data shows there is resounding support from parents and educators for content moderation to help keep students safer.

> ***More than 91% of Morning Consult survey respondents believe it is necessary to have online educational technologies in place to prevent students from accessing harmful or explicit content.***

- **More than 91% of survey respondents** — including parents, teachers, and administrators — **believe it is necessary to have online educational technologies in place** to prevent students from accessing harmful or explicit content.
- Of those, **over 95% reported it is a school's responsibility** to put these tools in place.
- Additionally, **nearly 90% of all respondents are supportive of online educational technology that could help detect signs of a student considering harming themselves or others.**

Schools recognize their role in protecting students' safety in the digital environment and understand that they operate in a complex student privacy policy framework.

Protecting Student Privacy Rights

At the federal level, two policies establish the balancing act schools need to walk: on the one hand, the Children's Internet and Privacy Act (CIPA) mandates that schools monitor students' online activity in order to receive federal E-rate funding, while on the other hand, the Family Educational Rights and Privacy Act mandates that schools safeguard the personal student data to which they maintain.

Since 2014, 49 states have also introduced over 500 student privacy bills, with at least 100 bills introduced each year, regulating how school systems, state education agencies, and technology providers handle student data.[3]

> ***More than 83% of those polled indicated they trust their school system to make informed decisions about which online technologies are appropriate for school use.***

To show their commitment to protecting student privacy rights, many companies — including GoGuardian — have obtained external validation from groups like iKeepSafe to demonstrate their commitment to safeguarding personal student information.

But protecting student privacy isn't just the concern of edtech companies and policymakers — it's top of mind for schools as well. Data shows that just like parents trust schools to keep students safe during the school day, they also trust them to protect student privacy.

Schools and districts are in a precarious position when it comes to balancing student safety and privacy. On the one hand, they've been entrusted with protecting students from harmful content or harming themselves or others, but on the other, they have a vested interest in protecting student privacy as well.

In the same Morning Consult survey, respondents reported significant levels of trust in schools to come to the best decision regarding the use of technology.

- More than **83% of those polled indicated they trust their school system to make informed decisions** about which online technologies are appropriate for school use.
- **Ensuring student data is not shared or sold** was a key priority for survey respondents when measuring comfortability with online educational technologies.

Before schools deploy student safety or content filtering technologies, however, it's important school leaders consider how best to address both protecting student safety and safeguarding student privacy. GoGuardian's Hartman suggests that schools can balance these two interests while building trust with the community by taking a TACT-ical approach.

Try A Little TACT

When it comes to implementing school technology, Hartman, a parent and former educator himself, suggests school leaders start by focusing on four elements collectively known as TACT: Transparency, Access, Communication, and Teamwork.

Transparency

Transparency builds trust between a school and its community of students and families. In the context of deploying student safety or content filtering technologies, transparency means the school system publicly shares:

- Who the vendor is
- What types of data privacy protections do both the school system and vendor have in place
- When the technology will be active (e.g., time of day, nights, weekends, and vacations)
- Where the technology will be active (e.g., school-managed devices students can take home, school-based computers, and school-managed student accounts)
- How the technology generates alerts
- Why the school believes self-harm alerting technology is a critical part of its student safety and support program

Schools and districts should publicly share a list of all technology vendors, the data privacy protections each vendor (and the school) has in place, the specifics of when and on which devices the technology will be active, and how these technologies are used to support student safety. (For example, with GoGuardian, schools can activate the School Session Indicator, an additional layer of transparency that displays on any device being filtered or monitored.)

Access

By the nature of the technology, student safety tools will most likely contain sensitive student information — especially if the technology identifies students who may be actively planning to harm themselves or others. Schools should be cautious in deciding who can access sensitive student data, and parents and caregivers have a right to ask who has the authorization to view their child's information at the school and through the vendor. Because of this sensitive information, schools should be incredibly thoughtful in deciding who has access to the dashboards and notifications.

> ***Schools must be cautious in deciding who can access sensitive student data, and parents and caregivers have a right to ask who has the authorization to view their child's information at the school and through the vendor.***

In the case of student safety technology, school system leadership should work closely with their technology team to ensure qualified school staff and authorized school partners (such as a local mobile crisis team) trained in handling sensitive information are the only ones who can access alerts. In addition, if a school partner will be part of the notification process, then the school system should have an agreement in place with the partner that identifies both parties' responsibilities for handling sensitive student information in accordance with the Family Educational Rights and Privacy Act (FERPA).

Communication

Ongoing communication between the school system and its community of students and caregivers is essential to any successful edtech implementation. However, it's especially critical when implementing student safety and content filtering technology.

Before deploying student safety technology, schools should provide information on what caregivers can expect if their student's activity generates an alert. Schools should also consider providing resources for caregivers to learn more about warning signs for potential suicide or self-harm risk and how they can access help for their child.

Schools, parents, and caregivers can help by holding community dialogues about suicide and self-harm prevention and sharing tools to support better mental health. Additionally, schools should consider cultural differences regarding mental health and work with their communities to foster an ongoing dialogue with caregivers via multiple methods of communication (email, newsletters, town halls, webinars) in as many languages as relevant to the school community.

Teamwork

While technology can play a powerful role in helping schools protect students from harmful content and identify warning signs of a mental health crisis, schools must integrate the technology into a broader student support program. Ideally, schools should have two things in place as they begin to deploy the self-harm alerting technology: (1) clearly articulated protocols for how to handle a notification that a student may be actively planning an act of self-harm or suicide (ex: the Model School District Policy on Suicide Prevention), and (2) a team of mental health and counseling professionals trained both on the software and how to respond to alerts.

If schools do not have these in place already, onboarding and implementing this technology is a valuable opportunity for schools to create a support team and develop their response protocols.

Striking the Balance Requires Work

Navigating the complexities of student safety and privacy is no longer optional — the increase in student mental health struggles and proliferation of digital data demand both take priority. Schools are uniquely positioned to support student mental health and connect families with resources, but doing so requires a system-wide dedication to protecting student privacy.

We owe it to our children to take a balanced, nuanced approach to their privacy and safety. Finding the right balance takes intentional work — but it's work that is worthwhile. ■

A Proactive Approach to Privacy

GoGuardian recognizes the trust educators place in us — trust that our technologies help schools protect students' safety and that the company protects students' privacy.

As recognized leaders in student data privacy, GoGuardian is independently certified as FERPA compliant by iKeepSafe. Our dedicated Privacy Team works across all divisions of the company to implement proactive privacy protections. Learn more about GoGuardian's approach to student data privacy by exploring our Privacy & Trust Center.

Footnotes

[1] *Mars B, Heron J, Biddle L, Donovan J L, Holley R, Piper M, Potokar J, Wyllie C, Gunnell D. Exposure to, and searching for, information about suicide and self-harm on the Internet: Prevalence and predictors in a population based cohort of young adults. Journal of Affective Disorders. 2015; 185:239-245.*

[2] *Rones M, Hoagwood K. School-based mental health services: A research review. Clinical Child & Family Psychology Review. 2000; 34:223–241.*

[3] *"State Laws and Legislation." Student Privacy Compass, studentprivacycompass.org.*

Scale Security, Not Complexity

Explore GoGuardian's collection of purpose-built safety and security solutions for your students, staff, and sites. Visit goguardian.com/safety-security to learn more.

GoGuardian Admin™

K-12 Web Filtering

Filter and manage policies for school-issued devices and guest networks. This includes:

- Device inventory management
- Intuitive reporting dashboards
- Parent mobile app access

GoGuardian Beacon®

Student Safety

Support student safety by identifying online activity that indicates a risk of suicide, self-harm, or possible harm to others. This includes:

- Suicide and self-harm alerts
- Customizable escalation points
- Optional 24/7 review of alerts

GoGuardian

GoGuardian 2030 E Maple Ave El Segundo, CA 90245

twitter.com/goguardian | instagram.com/goguardian | facebook.com/goguardian | linkedin.com/goguardian