Student Success Requires Trust: Balancing Privacy and Security in Schools

We live in a world where everything is at our fingertips. We can look up a phrase that's on the tip of our tongue, learn how to make sourdough bread, get some work done while sitting beachside, have our weekly groceries delivered to our home, endlessly scroll through content the algorithm catered just for us — it doesn't end.

While many of us enjoy the multitudes in our pockets, just as many of us are concerned about the impact. It seems like our phones are listening to us, delivering ads for items we've talked about — or even those we swore we only thought about. And how exactly did social media know to show me the right blend of dog and recipe videos as I scroll?

Sometimes it feels like technology is reading our minds. While most adults today remember a time where we felt like technology wasn't powerful enough to invade our privacy, that's not true for the latest generation.

Young people have to face the looming surveillance of technology throughout their lives, whether they're conscious of this or not. Because the fact is, a lot of technology is watching. Platforms are building profiles based on your behavior to determine what content to deliver to you.

But it doesn't have to be this way. Everyone deserves privacy.

Watched students are stifled students

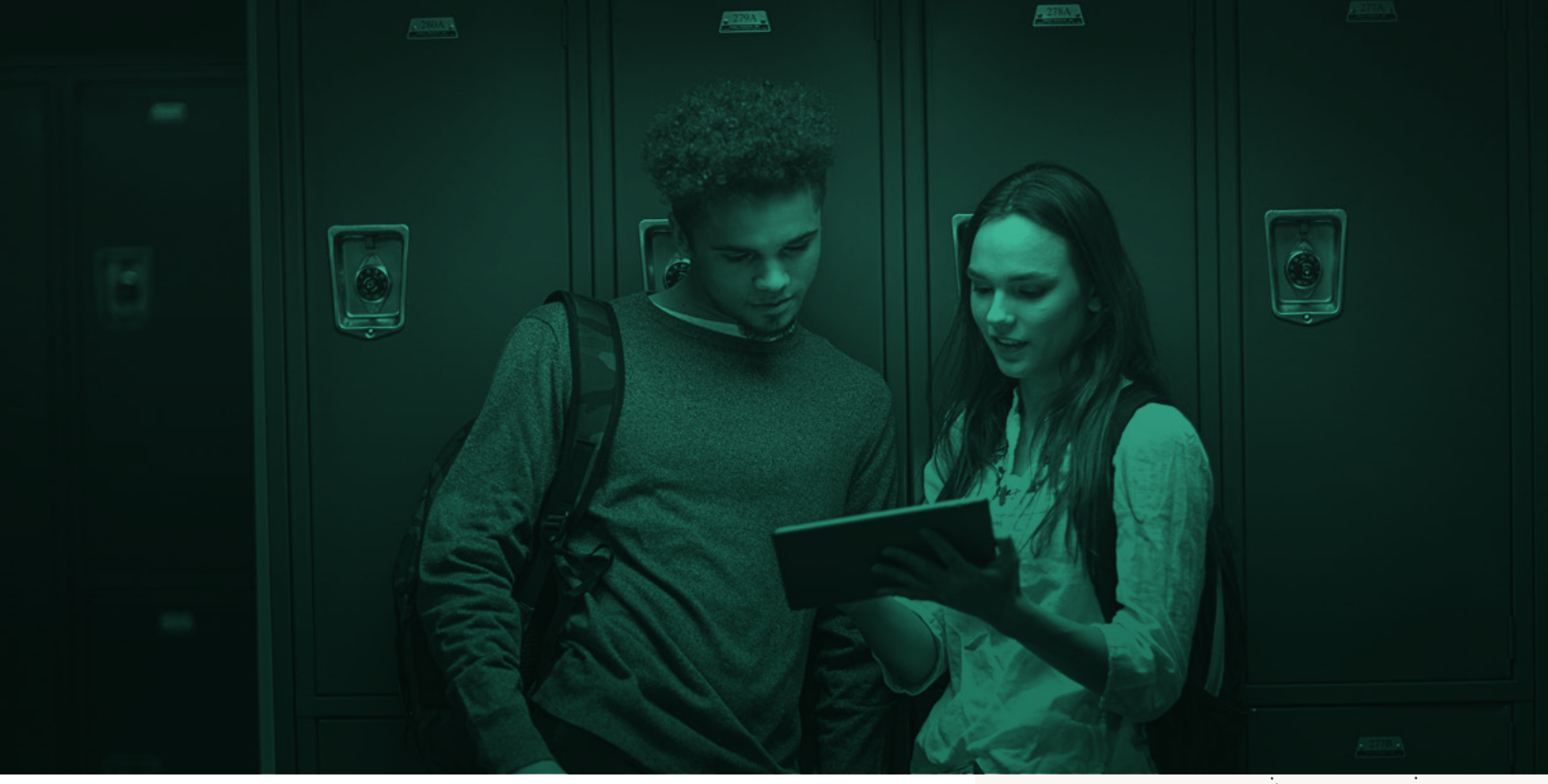
Students are in school for much of their young lives. This means schools have the responsibility to keep these students safe from a number of harms. Because technology is powerful, some administrations opt to watch what students are doing on their devices, recording their every move. **But does this actually keep anyone safer?**

It doesn't appear so. In fact, data suggests it seems to hurt student well-being. The Center for Democracy and Technology **reports that 60% of students** don't feel comfortable "expressing their true thoughts and feelings" online if their activity is monitored. This hurts their self-identity and creative expression, and technology can't catch any red flags **since they aren't being expressed anyway.**

An **article published in the North Carolina Law Review** outlines how low-income families are the most vulnerable to surveillance from their schools, leading to adverse, inequitable outcomes. After all, if a higher-income student wants to use a device without the prying eyes of their school, their family can afford to purchase their own device. The article also cites a **lack of evidence** that surveillance technologies improve learning outcomes and student safety. It also recalls so-called "success stories" where administrators intervened when a student expressed suicidal ideation — though without follow-up intervention, this may only teach the student to internalize their feelings because **their words are no longer private.**

This all creates an environment where **students don't trust the schools that are supposed to protect them.** It should come as no surprise that students don't feel safe when the devices that they use to learn and communicate with their peers are being watched. This is especially true when this could lead to encounters with the police. **Edsurge reports** that 70% of teachers say that their schools use surveillance technology for discipline, compared to 54% saying the tech is used to get students in front of a counselor, therapist or social worker. This means that students in trouble only receive help slightly over half the time while most schools are using tech for discipline. This disparity is troubling — after all, this technology supposed to help students, not punish them.

So where do we go from here?

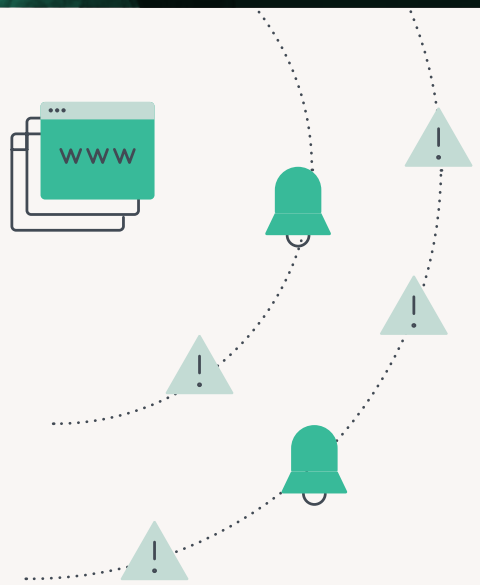


Technology is not a panacea

This is not to say that we have to go back to pencils and paper to be sufficiently private and secure. The problem with this surveillance approach is that it **uses technology as a catchall in the place of human interaction**. Technology cannot help a student with mental health issues or intervene if they are having problems at home. But it can help keep student and school data secure while blocking access to malicious or inappropriate content.

Using technology to monitor instead of surveil positions tech to securely support teaching and learning without teaching students that privacy-violating software is the norm. Think of **monitoring** like watching your kid play with their friends from afar; **surveillance** is invading their personal space and restricting their freedom to play as they please. Monitoring makes sure their devices haven't been compromised by attackers and protects them from harmful content — without helicoptering over them. Most of all, it doesn't unduly transfer the responsibility of protecting their well-being onto a soulless piece of software.

In our paper **Technology in Schools: Keeping Students Safe Without Surveillance**, we introduced this idea that when schools watch their students' every move, it takes way from student's well-being and security. This paper is going to focus on how to balance privacy and security while giving students confidence that their schools have their best interests in mind.



We'll discuss:

- Why a privacy-first attitude is a must
- Why fostering an environment of trust is important
- Technology's place in data protection and student safety
- Tools to support learning
- A strategy to balance privacy and security

Privacy is a right, not a privilege.

Schools don't just provide an education. They help students by:

- Providing them meals — including for students who can't always count on food at home
- Offering mental health and career counseling
- Giving them access to the internet, which they'll need to be familiar with after graduating
- Creating a stable environment with equity in mind

In other words, schools aspire to offer a safe place for students to land, with the intention of preparing them for life after graduation. While we can acknowledge that this is not a simple task with simple methods, I think we can agree that all students have the right to a fulfilling education. **Surveillance can hinder this fulfillment** if students don't trust the institution that intends to educate them.

What does that mean about privacy? Your average adult user is likely demanding that their information be kept private. We keep our phones locked for this very reason. So why should students — who schools are teaching to become successful adults — be held to a different standard?

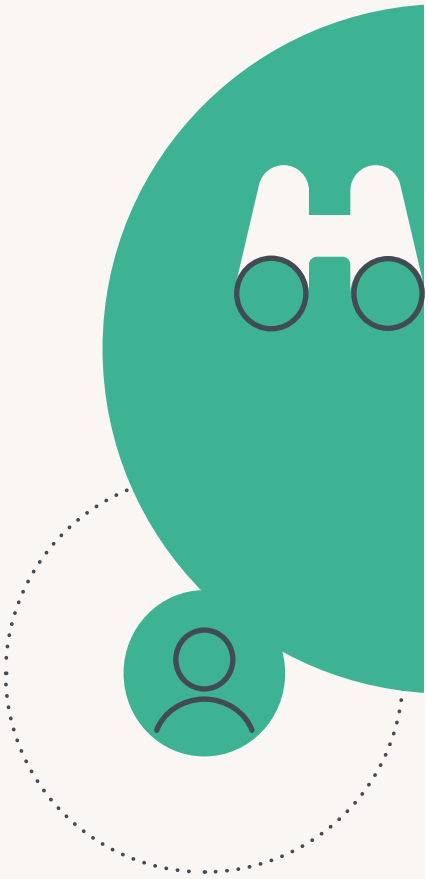
Because it's not easy to keep students safe — but as we've mentioned, technology isn't the answer. Instead, we can use tech to build up an environment where students can lean on it, when appropriate, and lean on the people around them when they're at their most vulnerable.

Cultivating trust helps students grow.

As much trust as we place in tech, we place more trust in our communities. Even the most sophisticated artificial intelligence can't impact our development more than the people around us.

This means that, at best, tech can only be a supporting role in our lives. And that the choices schools make surrounding technology impact students more than the tech itself does.

With intentionality and careful planning, technology can help build an environment where students can thrive. Successfully doing this requires schools and students to have a certain attitude towards tech.

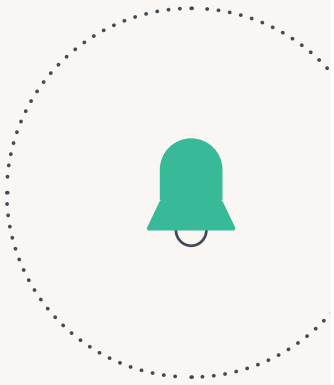


First, let's get a sense of how students and parents currently feel about surveillance. The Center for Democracy and Technology (CDT) **published a report** in 2023 that studies parents' experience with student activity tracking. Based on stories told by parents of children affected by surveillance, this report found that:

- Students **don't express themselves freely**, or explore topics related to identity in the fear of them being flagged.
- The flagging of inappropriate material "wasn't as significant as the actions that followed." Some students experienced **"mental and psychological impacts"** that don't fit the initial issue. For example, one school flagged a student who unknowingly received an email with gay pornographic content. Other students found out about the school's investigation, which eventually "led to the outing of the receiving child as gay, with significant consequences."
- "The **lack of privacy**" around flagged behavior and "the perception that students did something wrong," even when behavior related to school work was flagged, undermines their trust in the school and their teachers.
- When software triggers an alert, these are "not always kept private," which can **create a stigma.**
- Surveillance can "catalyze negative student behavior" and **directly threaten safety** and well-being.

The common thread here is that students don't trust technology, their teachers or their administration. This is the case regardless of a school's intent — because technology is so capable, it's easy to turn it into a tool for discipline. And the tools meant to help them end up causing harm. But an intentional implementation can reverse or prevent this sentiment.

Transparency and communication



Like many things in life, trust can be built with open communication. Schools should explain:

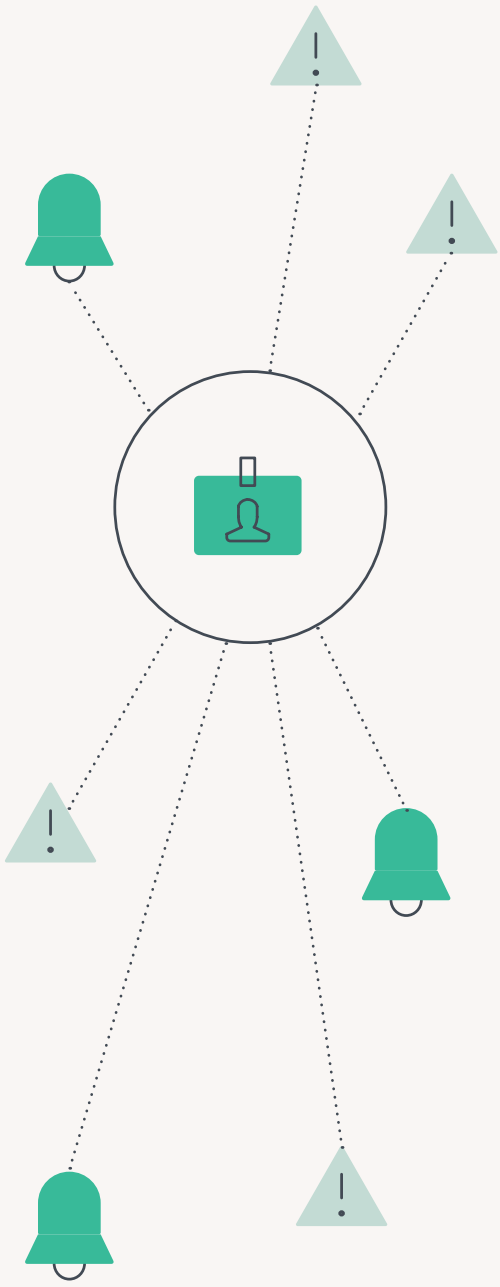
- Their policies and procedures surrounding tech use — what data is collected and how is it used
- How students can seek nonjudgmental support for issues related to mental health, identity and interactions with peers
- The dangers and benefits of technology use, especially applied to post-graduation

If schools are consistent about labeling tech as a tool for education — not discipline — students and parents can start building confidence that their technology use is for students' benefit.

When administrators choose to implement software in their schools, they can choose software that empowers educators and students without violating privacy. This is even true for devices owned by students and not the school. There's not a lack of this kind of software out there. Not to mention that using tech also teaches digital citizenship — how students will interact with technology going forward. If the tools they're offered teach them to:

- Take advantage of the host of resources the internet offers (within safety guardrails)
- Freely collaborate with their peers
- Recognize technology as a tool to help people, not to hinder them

... they're more prepared to safely and smartly use technology throughout their lives.



Protecting privacy and personal data

Technology doesn't sleep — which makes it perfect for 24/7/365 protection of data. Schools have legal obligations to protect student and employee data from third parties. It's not just data that's at stake; the loss of personally identifiable information (PII) can affect students beyond their time at school.

For example, as the **result of a 2020 data breach**, parents received notice that attackers tried to open credit cards and take out car loans using their elementary schoolers' information. These students are years away from trying to open their own credit cards to checking their credit scores — in the meantime, attackers could have used their data their own gain.

To help, the right software solutions can:

- Identify devices with a cyber threat and remediate the issue
- Monitor for unusual network activity that may indicate a cyber threat — without collecting private information
- Block access to malicious content and websites
- Create reports that help admins stay on top of their devices' health

When combining this software with user education, the risk to student data significantly lowers.

Jamf Safe Internet:
Privacy by design and default

At Jamf, we believe our software should improve the education experience for students, teachers and administrators alike.
This means:

- Supporting IT admins with simple but capable tools to manage and secure devices
- Helping teachers manage their classrooms
- Protecting students from dangerous parts of the internet
- Designing products with privacy in mind
- Knowing when software should support humans and not replace them

Privacy is at the heart of Jamf Safe Internet, our security software built specially for education. Jamf Safe Internet is designed to keep Apple devices, Chromebooks and Windows laptops free from security threats and students safe from harmful content — all without violating their privacy or creative expression.

"*Full Privacy*" is set by default, meaning that user and device information is pseudonymized and cannot be used to identify users. Admins are also able to enable "*Balanced Privacy*" to show user and device identifiers to associate certain devices to users for security threats. Anything related to content stays anonymous. This helps admins know who to reach out to in case a device shows signs of compromise and needs manual intervention or the user needs training.

Combined with our school-designed mobile device management software Jamf School, institutions can rest assured that their tech stack is working to keep their students safe. This means teachers can focus on their classrooms; students can focus on their learning and staff can provide the needed human support to help students thrive beyond the capabilities any tech alone could give.

Jamf School supports educational tech with:

- Simple deployment whether devices live on a cart, sit in a lab, are given 1:1 or are owned by students
- Dashboards to keep track of managed devices, users and apps at a glance
- Classroom management tools
- App request tools so teachers can easily request apps from IT
- Apps for students to have limited control over their devices

Jamf Safe Internet keeps students away from harmful content and devices free from compromise with:

- Powerful on-device content filtering fueled by machine learning — so even undiscovered threats are blocked*
- Best-in-class network threat prevention
- Content control to restrict access to certain categories, like social media
- The ability to mandate Google SafeSearch and YouTube Restricted Mode for safe browsing
- High compliance to data storage standards
- A low profile with high performance

*This feature is exclusive to iOS and iPadOS devices

All this with a privacy-first philosophy and the belief that tech is no replacement for the human element for student well-being.

Building your defense strategy

Implementing a defense strategy that guards student data and allows for free and safe browsing of the internet isn't easy. Especially when this is coupled with a desire to protect student well-being. Some considerations when building this strategy are:

1. How do you support students when they aren't on school-owned devices?
2. How could you provide support online without it getting blocked by filters?
3. What support system can students access in times of need? How can you build a system free of judgement and full of empathy?
4. How do you use technology in a way that protects privacy and student well-being?
5. How does security software reporting support your network and your students?
6. How does building an environment of trust between students and technology benefit them for life beyond school?

Key takeaways

- Student well-being worsens when schools use surveillance, especially as a means of punishment.
- Surveillance prevents student self expression and is often inequitable.
- Building an environment where students can trust their schools helps them thrive — and can't be achieved if they're being watched.
- Teaching smart technology use prepares students for life after graduation.
- Technology is best at supporting IT admins, teachers, staff and students, not as a replacement for human intervention.

To see how Jamf can help be a part of your technology, security, and content filtering solution, learn more at Jamf.com

Learn More