Technology in Schools: Keeping Students Safe Without Surveillance

Every school has a level of responsibility for the well-being and safety of its students. The topic of student safety is a broad term covering many different functional areas, largely left open to interpretation by the district or school that implements those student safety measures.

Schools are left to decide for themselves as to what extent they want to implement safety measure laws, from providing privacy-minded content filtering without data collection, all the way to installing keyloggers on school-issued devices and surveilling everything a student types, sends and receives.

The paper will explore

- The meanings of monitoring and surveillance
- The wider impact of the terms as they relate to education and student privacy
- Considerations when developing technology policies, providing an overview for institutions when it comes to making informed decisions on what needs to be done.

The Problem

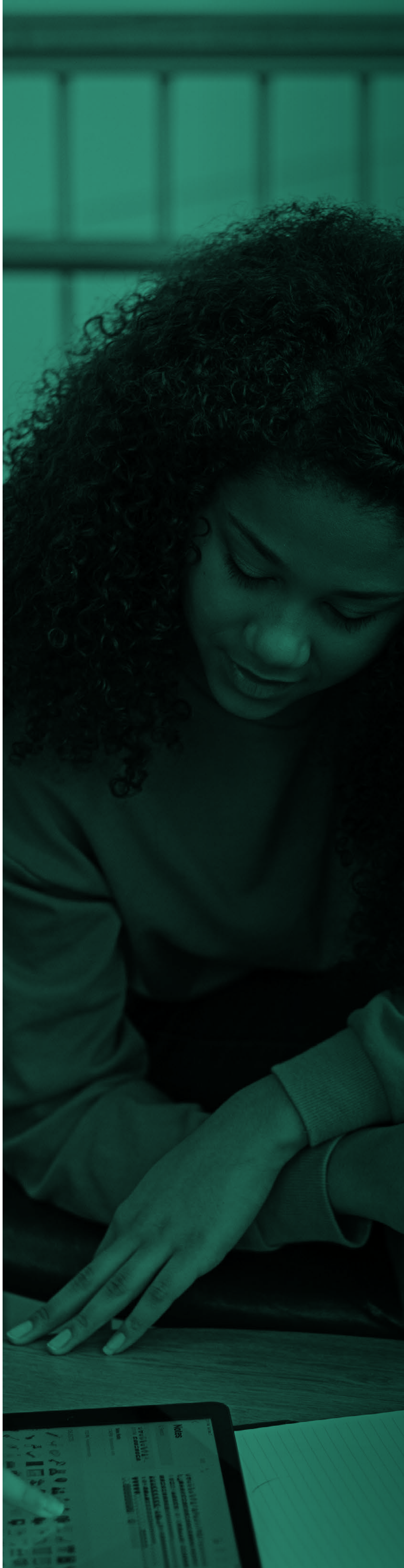
It takes a village: teachers, parents, healthcare professionals, school administrators, friends… the list goes on for the people who influence student's lives. On average, **United States students spend roughly one thousand hours per year**, across 180 days, in school. This puts teachers and other administrators as key influencers in students' lives, affecting issues around education, mental health, technological stewardship, general well-being and beyond.

Schools are cracking down on student internet usage for the sake of student safety: some are going so far to check for profanity use, indicators of possible self-harm or violence, or bullying from or against their peers. Schools are only a part of students' lives—and some students use their own devices outside of school oversight—so how involved should schools be in checking on their mental and physical well-being? And how much of this should rely on their online presence? Unfortunately, there's no obvious answer.

The internet gives schools a lot of power to educate. The availability of student-specific educational approaches, limitless information and countless other resources supports student learning in our information-heavy world. But of course, with this power comes the responsibility to consider how students interface with the content available online, some of which is inappropriate or dangerous.

Education goes beyond leveraging online knowledge. Schools want to empower students to be independent and responsible internet stewards while ensuring their safety and security. Since there's not a clear way to balance these concepts, there is a spectrum of approaches when it comes to student safety online. At one end, do we simply inform the student about safe and appropriate use while throwing them into the open internet to explore? Or do we lock it down so students can only access what we want them to access, meaning all sites have been pre-checked and are known to be safe?

These two ends of the spectrum showcase the range of issues that exist in education: freedom to explore vs. restrictive access. So what lies between these areas—what if we allow some freedom to explore while keeping an eye on students so they don't become overwhelmed? Does either side of the spectrum actually solve the issue with student safety, or are there better alternatives? How can we keep students safe holistically, even beyond the bounds of their school rules?



Understanding different approaches

Let’s discuss some approaches regarding how to handle student data. The first is **monitoring.**

Monitoring

Monitoring student internet usage collects data about the sites students access, when they access them and for how long. This data can give institutions a pattern of access about:

- What types of material students look for?
- What time of day is content being searched for — in or out of school hours?
- What material do students spend the most time on?

Monitoring focuses on the *data* rather than the students themselves—it considers the websites being accessed rather than who is accessing them. This gives schools insight into the general behavior of their student body and allows them to react to potential issues.

There are 3 common methodologies for how monitoring can be achieved:

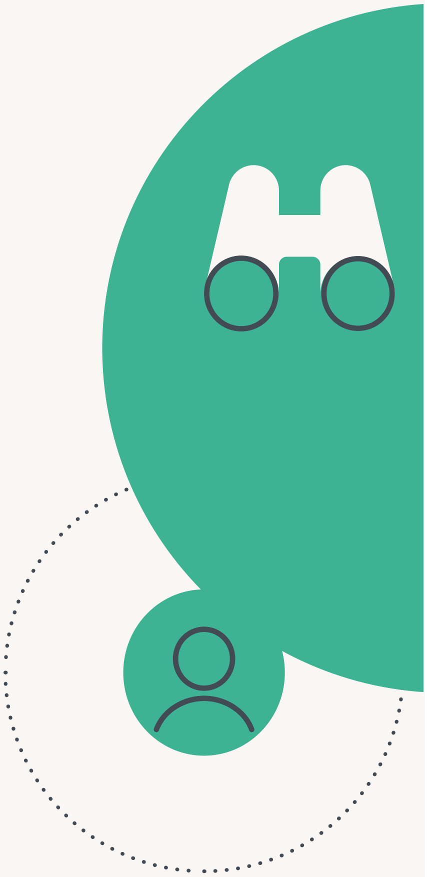
In person:
Monitoring student progress is an integral part of an educator’s role, but in-person methodologies can be time-consuming. Utilizing tools like Apple Classroom can aid in this task while fostering student education on appropriate use and maintaining a human connection to gauge their well-being. Monitoring in this way is an extension of an educator’s role in the classroom to support learning progress.

Technology monitoring
This includes tracking general online behavior, identifying potential risks or inappropriate content, and intervening when necessary to mitigate harm. The goal is to create a secure digital environment where students can learn and explore safely. But schools must draw a line to ensure they are also respecting privacy and autonomy. Schools can identify patterns of searches and use it to educate groups of students as part of a digital citizenship program.

Full-tech takeover
(which we cover in Surveillance below):
Technology tracks the student’s every move online and reports if they do anything against a policy. It’s often viewed as a ‘quick and easy’ solution but exposes schools to issues around false positives and snooping on students that, inevitably, reduces trust. This approach doesn’t take into account that students may have access to non-school-owned devices and doesn’t result in educated users.

Depending on how the data is collected and stored, the harvest of personally identifiable information (PII) can be reduced to protect student privacy while still maintaining valuable insight for institutions. Collecting anonymous data can also mitigate the amount of PII lost in a data breach, an increasingly common event for schools.

The second is **surveillance.**



Surveillance

Surveillance takes monitoring further by associating data to individuals, often in order to identify inappropriate behavior in real-time. This can look like recording an individual's search history, analyzing their keystrokes or looking in their private messages. While some districts only implement this on school-owned devices, some are also monitoring public student behavior **on social media.**

Surveillance can catch harmful student behavior before they become dangerous to others or themselves, hence why some school districts aim for this approach. But implementing this in a way that doesn't violate student privacy, create student **distrust in their institution**, create false positives for non-threats or **disproportionately target certain demographics** can be very difficult.

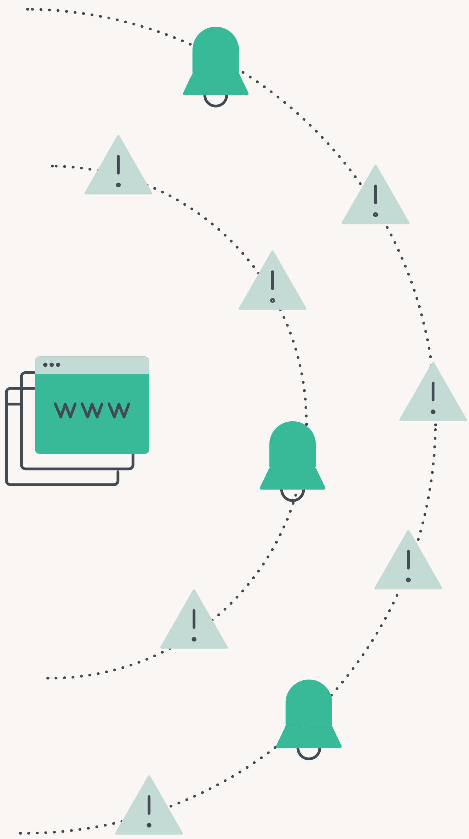
According to a recent **Center for Democracy and Technology (CDT) report**, 44% of teachers say they know a student who has been contacted by law enforcement based on data taken by their school. **And 29% of LGBTQ+ students report** that they or someone they know has been outed by this technology.

It's undeniable—surveillance is affecting every aspect of students' lives, not just at school. Adults wouldn't tolerate this level of scrutiny, so why are we teaching students that this is the status quo?

More data, more problems

Many of the companies in the student safety space offer a range of services that rely on having access to intimate levels of personal student information. The collection of that information and the ways that it is used creates a number of issues.

The first is that there is a privacy inequity for students in lower income brackets. Students that don't have access to a personal device and can only use the school-issued device are subject to an increased level of surveillance. Students with higher-earning guardians have the option to use their own personal devices like an iPhone or iPad to preserve their privacy. A 2020 McKinsey report examining the effect of remote learning on students found that ~9% of students don't have regular access to the internet at home, with Black and Hispanic 3-4% less likely to have access. The creeping inequalities in technology can create these demographics to be more susceptible to surveillance, meaning these groups can become disparate targets for the consequences of monitoring.



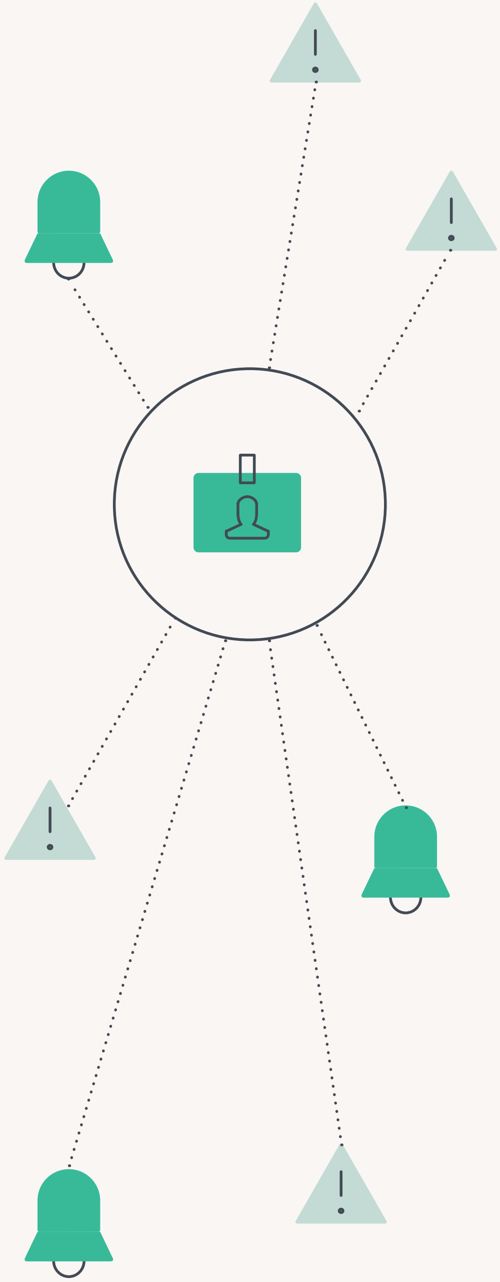
Educators say monitoring tools help them identify youth who are struggling and get them the mental health care they need at a time when youth depression and anxiety are spiraling. However, the results of a national survey by the nonprofit Center for Democracy and Technology (CDT), suggests an alternate reality: instead of getting help, many students are being punished for breaking school rules. And in some cases, survey results suggest, students are being subjected to discrimination. This again begs the question—is technology actually helping students?

Despite mixed opinions and practices from different schools, one thing seems clear: technology alone isn't enough. In the realm of education, it's increasingly apparent that relying solely on technology to address complex issues falls short of safeguarding students effectively. Placing undue faith in school-owned safeguards overlooks the broader context of student experiences, leaving them vulnerable and often resorting to personal devices. Recognizing the complexity of these situations, it becomes clear that a balanced approach—one that integrates technology with human intervention and support—is essential. By fostering open dialogue and prioritizing education and empathy, schools can create safer environments where students feel valued and empowered to navigate the digital landscape responsibly.

Digital citizenship is vital for students as they increasingly use technology in school and personally. It's crucial to consider personal internet use, ensuring students remain aware of online opportunities and risks after leaving school. While schools constantly educate on behavior change, relying solely on technology for analysis and reporting shifts problems elsewhere, potentially exposing students to greater harm.

So does drastic surveillance measures lead to drastic safety improvements? It turns out the effectiveness of the capabilities "unlocked" by collecting all this data is both poor and increases the legal exposure of the schools that choose to implement them. The detections are implemented using a set of keywords that will generate an alert if matched against. These generate an enormous number of false positives, but the school still has a responsibility to act on each alert.

These alerts, if real, can be telling of a potential issue with a student. But they often aren't the first sign of trouble. What can be more telling are aspects humans are more likely to spot first—the student's general demeanor, appearance, academic performance, level of engagement with peers, mood, attendance and more. Relying on technology to catch students in a bad place can be ineffective or too late.



Prevention over inspection

Many schools want to ensure students are browsing the internet safely by restricting access to inappropriate sites that contain material about gambling, adult content, gaming or other sites that are just not appropriate in an education setting. Content filtering can prevent this, stopping students from accessing this content in the first place. This approach leans more toward free access to the internet with some safety built in. Institutions can feel assured that students have freedom to explore, but in a more controlled environment that limits their access to anything potentially harmful.

Knowing that content filtering is in place and harmful content is unavailable to students can potentially negate the need to inspect what websites students are looking at. This goes back to the student privacy issue: should institutions look at everything a student is doing, or simply explore if the need arises due to a concern over a student's well-being?

By being proactive in blocking access to certain sites or content areas, institutions are able to use the internet to support learning and teaching in the everyday classroom setting, meaning students can develop their knowledge around the content being explored in the curriculum, without having access to anything they shouldn't. With certain tools, the internet can be highly restricted to only a handful of approved sites, or can be more open to approved categories. From a classroom perspective, it means learners are able to learn in their own way, explore knowledge from different sources and understand how the internet works for their benefit. In other words, students are able to not only learn the material relevant to their coursework, but how to be good digital citizens—valuable behavior for the rest of their lives.

A more reactive approach would be to analyze what is being looked at and then intervene with the learners, though this does mean that that content has already been surveilled. This would require someone in the institution to look through the data to see what has been looked at to then deal with that after the event, demanding specialized personnel and IT support.

The solution?

The UN Convention for the Rights of the Child lays out **this guidance related to child privacy:**

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation.

2. The child has the right to the protection of the law against such interference or attacks.

While this provides an excellent principle for protecting children's privacy, it doesn't provide explicit guidance for how to implement a balanced technology policy that keeps students out of danger. Students are not able to claim exemption from school surveillance on school-owned devices because of their "right to privacy," and therefore have little to no control of how their school handles their information. This can even extend to personal devices on school networks that are made susceptible to acceptable use policies (AUPs) stating data will be harvested. In other words, students have no choice in how their schools collect their data, especially affecting students without access to data plans or their own devices at home.

Consequently, institutions are forced to come up with their own policies and procedures based on their perception of student safety. After all, danger is coming from a variety of sources: internet sites, their peers, even themselves. Schools are forced to respond to pressure from their communities and often feel the burden to prevent the worst-case scenario—the loss of a student's life.

Technology is not a panacea

So the question is, what should schools actually do? Again, it takes a village, and technology alone cannot keep students safe. Students have to navigate the content on the internet, relationships with their family and friends, their own mental health and identity and their living situations at home. School counselors, teachers, healthcare professionals and school administrators still need to have critical relationships with students to determine a student's well-being. Technology should only be a part of the solution, rather than overtake a student's entire life. Surveillance should considered when there's a need to closely examine a student who has been identified as a risk by professionals, rather than as a default for the student body. After all, once a student graduates, they have the entire internet to explore; if schools lockdown the web, are students going to be prepared for any potential threats the internet has to offer?

Good content filtering can limit distractions and dangers while students are still in schools, without making them feel like everything they say, do or think is being scrutinized for misbehavior (and therefore punishment). And content filtering on your school networks and devices doesn't care about the student's family income or demographics, lessening the inequalities certain groups may face.

Beyond content filtering, schools should follow cybersecurity best practices to protect any data they do collect. This includes:

- Having clear account provisioning and access controls for student accounts
- Using strict access controls for any devices and applications that have access to student information
- Developing a clear plan in case of a cyber attack
- Securing endpoints with endpoint detection and response (EDR) software
- Taking regular data backups in case of recovery
- Encrypting your data servers and devices
- Implementing security information and event management (SIEM) software
- Developing an appropriate training program to teach faculty, staff and students about the risks of an online presence

Key takeaways

- Schools have a responsibility to protect students from harmful internet content, but how closely student activity should be looked at is not clear
- Watching everything students do online can have a negative effect on their well-being
- School surveillance programs can discriminate against certain groups of students
- Observing a student's disposition can identify troubled students in ways technology can't
- Surveillance and monitoring should be carefully implemented as a partial solution for student safety
- Institutions should develop strong security policies to protect student data

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

Learn More