POLICY PAPER

Watched After the Bell

Guardrails for Student Monitoring Software in Virginia

Submitted to the Virginia General Assembly
for Consideration in the 2027 Regular Session

MANGO (Modern Advocates for New Global Opinions)
Richmond, Virginia
September 30, 2026

I. Executive Summary

Virginia should enact a law setting clear limits on how school divisions monitor students through school-issued devices and accounts. At present, no Virginia statute specifies when monitoring may occur, what it may scan, who must review an automated flag, or when a flag may be referred to law enforcement.

Most Virginia students complete their schoolwork on a division-issued laptop and a school Google or Microsoft account. Many divisions pair these with monitoring software that scans searches, email, documents, and chats, sometimes around the clock and inside the home. When the software flags content, an alert is sent to school staff and, in some cases, to law enforcement.

Virginia's student data laws focus on data security and on how vendors handle information. They do not address surveillance itself, and federal law (FERPA, COPPA, and CIPA) does not fill that gap. Meanwhile, no comprehensive independent study shows that broad monitoring prevents suicide or school violence. National surveys show that false alarms are common, that students self-censor when they know they are watched, and that the consequences fall most heavily on LGBTQ students, students of color, low-income students, and students with disabilities.

MANGO does not ask the Commonwealth to ban school safety tools. We ask for the following guardrails:

1. **Transparency.** Divisions publish the tools they use, what those tools scan, and annual aggregate counts of alerts and outcomes.
2. **No monitoring after hours,** except for device security, a student's own request for help, or a documented emergency.
3. **Human review first.** A trained staff member reviews context before any discipline, risk designation, or police referral. An automated flag alone is never grounds for a referral.
4. **No webcam, microphone, keystroke, or location surveillance** outside a narrow exception for lost or stolen devices.
5. **Deletion deadlines** for alerts and raw monitoring data.
6. **Plain-language notice** to students and parents, with a clear complaint process.

These measures preserve the legitimate safety benefits of these tools while ending their overreach. They carry little cost and give parents, students, and legislators information they currently lack. Draft bill language appears in Appendix A.

II. Statement of the Problem

A Virginia high school student's school laptop can be monitored in their bedroom at midnight by software their family may not know exists. That is the core of the problem this paper addresses.

Monitoring is close to universal. In a 2022 national survey by the Center for Democracy & Technology (CDT), 89 percent of teachers reported that their school uses student activity monitoring software (CDT, Hidden Harms). One vendor alone, GoGuardian, has reported serving approximately 27 million students.

The software does far more than block websites. It can read the content students write, flag it with automated tools, and route alerts to administrators. According to CDT's survey:

- **44 percent** of teachers reported that a student at their school was contacted by law enforcement because of monitoring.
- **37 percent** of teachers at schools that monitor after hours reported that law enforcement directly receives alerts flagged outside school hours.
- **29 percent** of LGBTQ+ students reported that they or someone they know was outed by the technology.

A 2023 follow-up found that approximately two-thirds of teachers at monitoring schools reported students being disciplined because of an alert (CDT coalition letter).

A. Use in the Richmond Region

Richmond-area school divisions use these tools. In 2018, WTVR reported that Chesterfield County Public Schools implemented Gaggle to scan students' Google files for concerning images and keywords. Reporting has also connected Henrico County Public Schools to GoGuardian on school-issued devices. What divisions use today, how those products are configured, and how many alerts they generate is not publicly reported. MANGO is requesting these records from Richmond-area divisions under the Virginia Freedom of Information Act and will share the results with the General Assembly.

B. The Student Perspective

Students are not asking to conceal genuine danger. They are asking for what adults already expect: to know when they are being watched, by whom, and what happens next. Virginia law does not currently require any division to answer those questions.

III. How the Technology Works

Monitoring software operates on the school device, the school account, or the school network, and it continues to function wherever the device travels unless the division limits it. Most products combine several of the following access points:

- A browser extension on a school laptop that logs searches and websites visited.
- A cloud connection to Google Workspace or Microsoft 365 that can read school email, documents, chats, and calendars.
- A network or web filter that blocks and logs internet traffic.
- Classroom management tools that allow teachers to view and control student screens in real time.
- An automated "safety" classifier that scores content and sends alerts to school staff or to the vendor's own review team.

In this market, "artificial intelligence" typically refers to keyword lists, rule-based categories, image recognition, and machine-learning scores, sometimes reviewed by vendor staff. These systems are not validated clinical or threat assessment tools.

Vendor	What It Can Monitor	When It Operates	Where Alerts Go
GoGuardian	Browsing, searches, documents, videos, extensions, live screens	Depends on district settings; can extend off campus	Designated school staff; police referral is a local decision
Gaggle	School email, documents, calendars, chats	Advertises around-the-clock alerts	Designated school leaders, after vendor staff review
Securly	Web filtering, classroom management, safety alerts	Depends on module and settings	Designated school contacts
Lightspeed Systems	Web filtering, device management, safety alerts	Device-based filtering can run off campus	District staff or vendor safety team
Bark for Schools	School Google and Microsoft accounts: email, documents, chat	Whenever school accounts are in use	District-designated contacts
Linewize / Qustodio	Web filtering, classroom visibility, wellbeing tools	Can run at home if enabled	School-defined recipients

Table descriptions are drawn from vendor materials and advocacy research. The configuration used by any individual Virginia division depends on its contract, which is why disclosure matters.

A. Six Distinct Practices

The term "monitoring" covers practices with very different privacy implications, and sound legislation should treat them differently:

1. **Network filtering:** blocking sites on the school network, required in some form for federal E-Rate funding.
2. **Device filtering:** blocking or logging on a school device wherever it is used.
3. **Cloud account scanning:** reading or scoring the contents of school email, documents, and chats.
4. **Classroom screen viewing:** a teacher viewing student screens during class.
5. **Ambient surveillance:** webcam, microphone, screenshots, keystrokes, or location.
6. **Safety alerts:** automated flags for self-harm, violence, bullying, drugs, or sexual content.

The danger of ambient surveillance is not hypothetical. In *Robbins v. Lower Merion School District* (E.D. Pa. 2010), a Pennsylvania district remotely activated webcams on school laptops inside students' homes and captured thousands of images and screenshots. The district settled for $610,000.

IV. Current Law and Its Gaps

Virginia regulates how student data is secured and shared. It does not regulate how students are watched. This bill addresses that gap.

A. Virginia Law

Va. Code § 22.1-289.01 (school service providers and school-issued devices). Enacted in 2015 (HB 1612) and expanded since, this section applies to school service providers, school technology providers, and school-issued devices. Providers must disclose what student personal information they collect and how they use it, maintain a privacy policy, allow students and parents to access and correct data, delete data upon a school's request, and refrain from selling it. It is a sound vendor-conduct statute, but it is silent on when monitoring may run, what content may be scanned, who reviews a flag, and when police may be involved.

Va. Code § 22.1-20.2 (student data security). Directs the Department of Education, with the Virginia Information Technologies Agency, to maintain a model data security plan addressing access controls, audits, breach response, and retention. This is guidance on protecting data, not a limit on collecting it.

Va. Code § 22.1-287.02 (students' personally identifiable information). Governs the protection and sharing of state-level student data.

Virginia Consumer Data Protection Act (Va. Code § 59.1-575 et seq.). Grants consumers rights to access, correct, and delete personal data, but exempts data covered by FERPA. Most school monitoring data therefore likely falls outside its protection.

B. Federal Law

Law	What It Does	Does It Limit Monitoring?
FERPA	Protects education records and limits their disclosure	No. It governs sharing, not collection or scanning.
COPPA	Requires consent for online data collected from children under 13	Minimally. It does not reach high school students, and schools may consent on families' behalf.
CIPA	Requires filtering of obscene or harmful images as a condition of E-Rate funding	No. It requires filtering, not scanning of student writing or after-hours surveillance.
PPRA	Requires consent for certain surveys on sensitive topics	Unclear. Passive scanning is not a survey.

The Fourth Amendment applies in public schools, but in modified form. In *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), the Supreme Court held that school searches must be reasonable at their inception and in their scope. The Court has never addressed continuous, suspicionless, automated scanning of every student's writing, including at home. That is precisely the kind of question a legislature should answer rather than leave to litigation.

C. Gaps in Current Law

1. No limit on monitoring outside school hours or off school property.
2. No distinction between filtering websites and scanning what students write.
3. No prohibition on remote webcam, microphone, keystroke, or location surveillance.
4. No requirement that a person review an automated flag before action is taken.

5. No safeguards on referring flags to police or school resource officers.
6. No public reporting of which tools divisions use or what they produce.
7. No deletion deadline for monitoring data and alerts.
8. No protection for sensitive personal information such as health, identity, or religion.
9. No notice or complaint process specific to monitoring.
10. No requirement to demonstrate effectiveness, measure false alarms, or assess bias.

V. The Evidence

The case for broad monitoring rests on a promise of safety that the public evidence does not yet support, while its costs are well documented.

A. False Alarms Are Common

The Electronic Frontier Foundation reviewed GoGuardian alert records obtained through public records requests and found that false positives heavily outweighed accurate identifications of harmful content, including flags on ordinary educational material. No vendor publishes independently audited accuracy rates, and no state requires them to.

B. Monitoring Is Used More for Discipline Than for Safety

In CDT's 2022 survey, 78 percent of teachers at monitoring schools reported that students had been flagged for disciplinary action, compared with 54 percent who reported students flagged for possible harm to themselves or others (CDT, Hidden Harms). A tool marketed as suicide prevention is functioning largely as a disciplinary tool.

C. Students Stop Speaking Freely

In a CDT survey, 58 percent of students at monitoring schools agreed with the statement, "I do not share my true thoughts or ideas because I know what I do online is being monitored" (CDT). Approximately 80 percent reported being more careful about what they search. The risk is greatest for the students who most need help: a student who fears that a search about depression or abuse will draw adult attention may not search at all.

D. The Burden Is Not Shared Equally

- **LGBTQ+ students:** 29 percent reported that they or someone they know was outed by monitoring software (CDT, 2022); CDT's 2023 survey found 19 percent.
- **Students of color and low-income students:** CDT reports that Black and Hispanic students experience disproportionate harm, and teachers report greater negative effects on low-income students.
- **Students with disabilities:** special education teachers were more likely to report students getting in trouble or being contacted by police because of monitoring.

E. Does Monitoring Prevent Harm?

Vendors cite cases in which an alert led to a timely intervention, and those cases matter. However, no comprehensive independent study demonstrates that broad monitoring reduces suicide, self-harm, or school violence. Stated fairly: monitoring may sometimes surface a genuine warning sign, but there is no public evidence that scanning every student's accounts around the clock is what keeps students safe.

F. Parents Share These Concerns

Parental support for monitoring has declined. CDT found that 71 percent of parents are concerned about schools tracking their children's location, and a large majority are concerned about their children's data being shared with law enforcement. According to CDT research cited in the Stanford Law Review, one in five parents do not know whether their child's school uses monitoring software at all (Citron, The Surveilled Student).

VI. Response to Arguments for Monitoring

School leaders who use these tools want to keep students safe, and this proposal allows them to continue doing so. Each major argument for monitoring has an answer that preserves the safety benefit while removing the overreach.

Argument for Monitoring	Why It Carries Weight	How This Proposal Responds
It prevents suicide and self-harm	Speed can matter in a crisis	Preserves an emergency pathway and routes flags to counselors first, with a trained person reviewing context
It prevents violence	Schools face pressure to identify threats early	Preserves threat assessment; prohibits treating an algorithmic flag alone as grounds for a police referral
It stops cyberbullying	Bullying occurs on school platforms	Permits monitoring of school platforms during school activities, with notice
Federal law (CIPA) requires it	E-Rate funding requires internet filtering	CIPA requires filtering harmful images, not reading student writing at midnight; the proposal protects filtering
Teachers need classroom control	Students go off task	Permits live screen viewing during class periods
Schools face liability	A missed warning sign could lead to litigation	Written protocols, human review, and documented response are a stronger legal position than unreviewed mass scanning
Parents want to be informed	Some families welcome alerts	Provides parents clear notice while recognizing that some disclosures can place students at risk

A. Anticipated Concerns

Likely skeptics include monitoring vendors, some school boards and superintendents, division technology and legal staff, and some school safety advocates. MANGO intends to consult these

stakeholders early, ask what a workable version looks like from their perspective, and adjust accordingly. The goal is legislation that divisions can readily comply with, not one that forces a choice between safety and the law.

B. Fiscal Impact

Most provisions require policy changes and reporting rather than new spending. Vendors already generate the alert counts and configuration settings this proposal asks divisions to disclose. The principal new cost is staff time for an annual report and for human review, which many divisions already perform.

VII. Recommendations

MANGO respectfully recommends that the General Assembly adopt the following eight guardrails, drafted in Appendix A as an addition to Title 22.1 of the Code of Virginia:

1. **Public inventory and annual report.** Each division publishes every monitoring, filtering, and classroom management product it uses, what each scans, whether it operates off campus, who receives alerts, and its retention schedule. Each year it reports aggregate counts of alerts by category, alerts closed with no action, counselor referrals, disciplinary actions, and police referrals. No student-identifying data is published.
2. **No monitoring outside school hours.** Scanning of student content is limited to the instructional day and school-sponsored activities, with exceptions for device and network security, a student's own request for help, and a documented, credible, and imminent threat.
3. **Human review before action.** A trained staff member reviews full context before a flag leads to discipline, a parent notification, a risk designation in a student record, or contact with police. An automated flag alone is never grounds for a law enforcement referral.
4. **Police referral safeguards.** Referrals based on monitoring require written approval by a principal or designee, except in an emergency, and are included in the annual report.
5. **Prohibition on ambient surveillance.** No remote activation of cameras or microphones, keystroke logging, or location tracking, except to locate a lost or stolen device.
6. **Deletion deadlines.** Alerts resulting in no action are deleted within 90 days. Raw monitoring data is retained no longer than necessary. At contract end, vendors delete data and certify deletion in writing.
7. **Notice and complaints.** Before issuing a device or account, divisions provide students and parents plain-language notice of what is monitored, when, and by whom, along with a complaint process.
8. **State model policy.** The Department of Education issues a model policy and publishes an annual statewide summary of division reports.

Together, these measures answer the questions every family should be able to ask: *What is being watched? When? By whom? And what happens to my child if something is flagged?*

VIII. Other States Have Acted

Virginia would not be the first state to act. Ohio, with a Republican legislature and governor, enacted limits on school device monitoring in 2024, demonstrating that this is not a partisan issue.

A. Ohio Senate Bill 29 (2024)

Ohio Revised Code § 3319.327, effective October 24, 2024, generally prohibits school districts and technology providers from electronically accessing or monitoring three features of school-issued devices:

- location tracking;
- audio or video recording, receiving, or transmitting; and
- student interactions with the device, including keystrokes and web browsing.

Monitoring is permitted only under enumerated exceptions, including a noncommercial educational purpose such as instruction, technical support, or exam proctoring with advance notice; a missing or stolen device; compliance with federal or state law; and participation in federal or state funding programs. In any year a district elects to monitor under an exception, it must provide written notice to parents. "School-issued device" is defined broadly to include accounts and software as well as hardware (Southern Local School District notice).

Virginia can adopt Ohio's default-off structure, its broad definition of "device," and its annual parent notice. Virginia can improve on Ohio by adding human review before police referral, public reporting, and deletion deadlines, none of which Ohio requires.

B. California SOPIPA (2014)

California's Student Online Personal Information Protection Act prohibits education technology operators from using student data for targeted advertising, building profiles for non-school purposes, or selling it. Virginia's § 22.1-289.01 already follows a similar model and provides a strong foundation on which to build.

States are moving from rules about how vendors store student data to rules about how schools watch students. Ohio has taken the first significant step. Virginia can take the next with a more complete framework.

Appendix A: Draft Legislation

The following is a working draft offered for a patron's consideration. Official text would be prepared by the Division of Legislative Services, and the section number below is a placeholder.

COMMONWEALTH OF VIRGINIA
2027 SESSION

A BILL to amend the Code of Virginia by adding in Article 5 of Chapter 14 of Title 22.1 a section numbered 22.1-289.02, relating to student activity monitoring on school-issued devices and accounts.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Article 5 of Chapter 14 of Title 22.1 a section numbered 22.1-289.02 as follows:

§ 22.1-289.02. Student activity monitoring; limitations; transparency.

A. As used in this section, unless the context requires a different meaning:

"Automated alert" means any notice, score, flag, or classification about a student generated in whole or in part by software, keyword matching, machine learning, or artificial intelligence.

"Instructional day" means the hours during which a student is scheduled to receive instruction or participate in a school-sponsored activity.

"School-issued device or account" means any hardware, software, application, or online account provided by a school division to a student for the student's use, including email, cloud storage, and communication tools.

"Student activity monitoring" means any electronic accessing, scanning, logging, analysis, or review of a student's content, communications, searches, browsing, or use of a school-issued device or account by a school division or by a school service provider or school technology provider acting on its behalf. "Student activity monitoring" does not include (i) network filtering required by federal law, (ii) measures necessary to maintain the security of the division's network or devices, or (iii) live viewing of student screens by a teacher during a class period in which the student is enrolled.

B. No school division or provider acting on its behalf shall conduct student activity monitoring outside the instructional day, except:

1. When a student or parent requests assistance;
2. When the division has a documented, reasonable belief that a student faces a credible and imminent threat of serious harm to self or others;
3. When required by a court order or warrant; or
4. To locate a school-issued device reported lost or stolen.

C. No school division or provider acting on its behalf shall remotely activate or access the camera or microphone of a school-issued device, record keystrokes, or track the location of a student through a school-issued device, except to locate a device reported lost or stolen or when required by a court order or warrant.

D. No automated alert shall be the sole basis for (i) disciplinary action, (ii) a notation in a student's scholastic record, (iii) notification of a parent that discloses a student's sensitive personal information, or (iv) a referral to a school resource officer or law-enforcement agency. Before any such action, a trained employee of the school division shall review the full context of the alert. An automated alert alone shall not constitute reasonable suspicion.

E. Except in an emergency involving an imminent threat to life or safety, no referral to a school resource officer or law-enforcement agency based in whole or in part on student activity monitoring shall be made without the written approval of the principal or his designee. Each such referral shall be documented.

F. Automated alerts that result in no action shall be deleted within 90 days. Other data collected through student activity monitoring shall be retained no longer than necessary for the purpose for which it was collected, consistent with the retention requirements of the Library of Virginia. Upon termination of a contract, a provider shall delete all such data and certify the deletion in writing to the school division.

G. No school division or provider shall use information obtained through student activity monitoring concerning a student's health, mental health treatment, disability, religious beliefs, political beliefs, sexual orientation, or gender identity for any purpose other than responding to a credible and imminent threat under subdivision B 2.

H. Before issuing a school-issued device or account, and annually thereafter, each school division shall provide students and parents with written notice in plain language describing (i) each monitoring product in use, (ii) the types of content monitored, (iii) the hours during which monitoring occurs, (iv) who receives alerts, (v) the division's policy on law-enforcement referrals, (vi) the retention schedule, and (vii) the procedure for filing a complaint.

I. Each school division shall publish on its website, and submit to the Department of Education, an annual report containing de-identified, aggregate data on (i) the monitoring products in use, (ii) the number of automated alerts by category, (iii) the number of alerts resulting in no action, (iv) the number resulting in counseling or mental health referral, disciplinary action, or law-enforcement referral, and (v) the number of alerts generated outside the instructional day. No report shall include information that could identify an individual student.

J. The Department of Education shall develop a model policy to assist school divisions in complying with this section and shall publish an annual statewide summary of the reports submitted pursuant to subsection I.

2. That the provisions of this act shall become effective on July 1, 2028.

3. That the Department of Education shall develop the model policy required by subsection J of § 22.1-289.02 of the Code of Virginia, as created by this act, no later than January 1, 2028.

Sources

- Va. Code § 22.1-289.01, School service providers; school-affiliated entities; school-issued devices; student personal information
- 2015 Acts of Assembly, Chapter 728 (HB 1612)
- Ohio Revised Code § 3319.327, Monitoring of school-issued devices
- Southern Local School District (Ohio), Notice under Senate Bill 29

- Center for Democracy & Technology, Hidden Harms: The Misleading Promise of Monitoring Students Online (2022)
- Center for Democracy & Technology, Hidden Harms: Targeting LGBTQ+ Students (2022)
- Center for Democracy & Technology, Student Activity Monitoring Software: Research Insights and Recommendations
- Center for Democracy & Technology, Beyond the Screen: Parents' Experiences with Student Activity Monitoring
- CDT and OTI Coalition Letter Summarizing 2023 Findings (May 2024)
- Danielle Keats Citron, The Surveilled Student, 76 Stanford Law Review 1439 (2024)
- *New Jersey v. T.L.O.*, 469 U.S. 325 (1985)
- *Robbins v. Lower Merion School District*, No. 10-665 (E.D. Pa. 2010)