

POLICY PAPER

Know What's Watching

A Proposed Student Activity Monitoring Policy

Submitted to the [Division Name] School Board
by Students of the Richmond Region

MANGO (Modern Advocates for New Global Opinions)

Richmond, Virginia

September 30, 2026

I. Summary

The [Division Name] School Board should adopt a policy that sets clear limits on student activity monitoring and tells families exactly how it works. The Board has full authority to do this now through local policy and vendor contract settings.

We ask the Board to take six steps:

1. **Publish** the monitoring tools the division uses, what each scans, and when.
2. **Turn off after-hours scanning** of student content, except for emergencies and device security.
3. **Require human review** before any automated flag leads to discipline or police contact.
4. **Prohibit** remote camera, microphone, keystroke, and location tracking.
5. **Set deletion deadlines** for alerts and monitoring data.
6. **Report annually** on alerts and outcomes, with no student-identifying information.

These steps protect students without removing any tool the division needs to keep them safe.

II. Why This Matters to Our Students

Monitoring software is in nearly every school. In a 2022 national survey by the Center for Democracy & Technology (CDT), 89 percent of teachers said their school uses it ([CDT, Hidden Harms](#)). The same survey found:

- **44 percent** of teachers reported a student at their school was contacted by law enforcement because of monitoring.
- **37 percent** of teachers at schools that monitor after hours said law enforcement directly receives alerts flagged outside school hours.
- **78 percent** of teachers at monitoring schools reported students flagged for disciplinary action, compared with 54 percent reporting students flagged for possible harm to self or others.
- **29 percent** of LGBTQ+ students said they or someone they know was outed by the technology.

False alarms are common. The Electronic Frontier Foundation's review of GoGuardian alert records found that false positives heavily outweighed accurate flags of harmful content, including flags on ordinary schoolwork.

Students notice. In a CDT survey, 58 percent of students at monitoring schools agreed that they do not share their true thoughts or ideas online because they know they are monitored ([CDT](#)). The students most at risk are the ones most likely to stop searching for help.

Monitoring is already in use in the Richmond region. In 2018, WTVR reported that Chesterfield County Public Schools implemented Gagggle to scan students' Google files, and reporting has connected Henrico County Public Schools to GoGuardian.

III. Questions Families Deserve Answered

MANGO is requesting public records from [Division Name] under the Virginia Freedom of Information Act. Regardless of what those records show, we ask the Board to answer the following questions publicly:

1. Which monitoring, filtering, and classroom management products does the division use?
2. What do they scan: browsing, searches, email, documents, chats, or screens?
3. Do they operate after school hours, on weekends, or off campus?
4. Who receives alerts: teachers, administrators, counselors, vendor staff, school resource officers, or police?
5. Does a trained person review an alert before action is taken?
6. How many alerts were generated last year, and how many led to no action, counseling, discipline, or police contact?
7. How long is monitoring data kept, and is it deleted when a contract ends?
8. How are students and parents told about monitoring, and how can they raise concerns?

IV. What the Board Can Do Now

No state law is needed for any of the following. Each can be done through policy, administrative regulation, or vendor configuration.

A. Adopt a Policy

Adopt the policy in Appendix A as a new policy or as an amendment to the division's acceptable use policy for technology.

B. Review Vendor Settings

Most monitoring products let divisions choose which applications are scanned, which alert categories are active, which hours monitoring runs, and who receives alerts. The Board can direct staff to disable after-hours content scanning and limit alert recipients to trained staff.

C. Review Contracts at Renewal

When monitoring contracts come up for renewal, the Board can require vendors to provide aggregate alert reports, document their human review practices, and certify data deletion at contract end, consistent with the vendor duties already set out in [Va. Code § 22.1-289.01](#).

D. Update Referral Procedures

The Board can direct staff to update procedures, including any memorandum of understanding with local law enforcement for school resource officers, so that monitoring alerts go to counselors first and are referred to police only with an administrator's documented approval, except in emergencies.

E. Include Students

The Board can invite student representatives to review the division's monitoring practices each year and give feedback before contracts are renewed.

V. Anticipated Concerns

Concern	Response
Monitoring keeps students safe	The policy preserves emergency response and routes alerts to counselors first. It removes only practices without evidence of benefit, such as unreviewed after-hours scanning.
Federal law requires monitoring	CIPA requires filtering obscene or harmful images for E-Rate funding. It does not require scanning student writing or monitoring at home. The policy keeps filtering in place.
This creates work for staff	Vendors already generate alert counts and configuration reports. The annual report draws on existing data.
Liability if something is missed	Written protocols and documented human review put the division in a stronger position than unreviewed mass scanning.

Other jurisdictions have acted. Ohio enacted limits on school device monitoring in 2024, generally barring districts from monitoring location, audio and video features, keystrokes, and web browsing on school-issued devices except under listed exceptions with written notice to parents ([Ohio Revised Code § 3319.327](#)). MANGO is also asking the Virginia Board of Education for statewide guidance and the General Assembly for legislation. Local action now would make [Division Name] a model for the Commonwealth.

Appendix A: Proposed Policy

Student Activity Monitoring on School-Issued Devices and Accounts

Policy [Code]

A. Purpose. The [Division Name] School Board recognizes that technology helps keep students safe and supports learning, and that students and families have a right to know how that technology is used. This policy establishes limits and transparency for student activity monitoring.

B. Definitions. “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 the division or a vendor acting on its behalf. It does not include network filtering required by federal law, measures necessary to secure division networks or devices, or live viewing of student screens by a teacher during the student’s class period. “Automated alert” means any flag, score, or classification generated in whole or in part by software or artificial intelligence. “Instructional day” means scheduled instruction and school-sponsored activities.

C. Hours. The division shall limit student activity monitoring to the instructional day, except when a student or parent requests assistance, when the division has a documented, reasonable belief that a student faces a credible and imminent threat of serious harm, when required by court order or warrant, or to locate a lost or stolen device.

D. Prohibited features. The division shall not remotely activate cameras or microphones, record keystrokes, or track student location through school-issued devices, except to locate a lost or stolen device or when required by court order or warrant.

E. Human review. No automated alert shall be the sole basis for discipline, a notation in a scholastic record, a parent notification disclosing sensitive personal information, or a referral to a school resource officer or law enforcement. A trained employee shall review the full context first, and alerts concerning student wellbeing shall be routed to a school counselor or other student support staff.

F. Law enforcement referrals. Except in an emergency involving an imminent threat to life or safety, a referral based on monitoring requires written approval by the principal or designee and shall be documented.

G. Sensitive information. Information concerning a student’s health, mental health treatment, disability, religious or political beliefs, sexual orientation, or gender identity obtained through monitoring shall be used only to respond to a credible and imminent threat.

H. Retention. Alerts resulting in no action shall be deleted within 90 days. Other monitoring data shall be kept no longer than necessary, consistent with Library of Virginia retention schedules. Contracts shall require vendors to certify deletion at contract end.

I. Notice. Before issuing a device or account, and annually, the division shall give students and parents plain-language notice of each monitoring product, content monitored, hours of operation, alert recipients, referral procedures, retention schedule, and how to raise concerns. The notice shall be posted on the division website.

J. Annual report. The Superintendent shall present to the Board, and post on the division website, an annual de-identified report of products in use, alerts by category, alerts closed with no action, counseling referrals, disciplinary actions, law enforcement referrals, and alerts generated outside the instructional day.

K. Review. The Superintendent shall review this policy and the division's monitoring practices annually, with input from students, parents, and staff, before renewing any monitoring contract.

Adopted: _____

Sources

- [Va. Code § 22.1-289.01, School service providers; school-affiliated entities; school-issued devices; student personal information](#)
- [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)