POLICY PAPER

A Statewide Standard for Student Activity Monitoring

Recommendations to the Virginia Board of Education

Submitted to the Virginia Board of Education
and the Virginia Department of Education

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

I. Executive Summary

The Virginia Board of Education should adopt statewide guidelines for student activity monitoring on school-issued devices and accounts. Today, each division decides for itself when monitoring runs, what it scans, who reviews automated alerts, and when alerts reach police. Families have no consistent way to know.

Virginia law already gives the Department of Education this role. Va. Code § 22.1-20.2 directs the Department, with the Virginia Information Technologies Agency, to maintain a model data security plan covering access, privacy compliance, audits, breach response, and data retention. Va. Code § 22.1-20.2:1 calls for guidance on artificial intelligence systems in schools, including student data privacy in the context of those systems. Monitoring software is one of the largest sources of student data and one of the most common uses of AI in Virginia schools. It belongs in that framework.

MANGO asks the Board and the Department to take five actions:

1. **Adopt model guidelines** on student activity monitoring for school divisions (draft in Appendix A).
2. **Incorporate monitoring standards** into the model student data security plan (§ 22.1-20.2), the Department's AI guidance (§ 22.1-20.2:1), and the Model Policy Concerning Internet Safety.
3. **Recommend standard contract terms** for monitoring vendors in division data privacy agreements.
4. **Collect and publish** annual, de-identified statewide data on monitoring alerts and outcomes.
5. **Support legislation** codifying these protections in the 2027 Regular Session.

These steps require no ban on safety tools and little new spending. They give divisions a clear, defensible standard and give families the transparency they currently lack.

II. The Problem

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). 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 reported that 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 reported that they or someone they know was outed by the technology.

Monitoring software can read school email, documents, and chats, log every search, and in some configurations operate off campus around the clock. The "AI" in these products typically means keyword lists and machine-learning scores, not validated clinical or threat assessment tools. The Electronic Frontier Foundation's review of GoGuardian alert records found that false positives heavily outweighed accurate flags of harmful content.

Richmond-area divisions use these tools. In 2018, WTVR reported that Chesterfield County Public Schools implemented Gaggle to scan students' Google files, and reporting has connected Henrico County Public Schools to GoGuardian. No statewide data exists on how many Virginia divisions use monitoring, how it is configured, or what it produces.

The consequences reach beyond privacy. 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). A student afraid that a search about depression or abuse will trigger adult attention may not search at all.

III. Why the Board Should Act

A. The Department Already Has a Mandate

Va. Code § 22.1-20.2 directs the Department to develop and update, at least annually, a model data security plan for student data and to make it available to every division. That plan must address access, privacy compliance, audits, breach response, and retention. Monitoring data is student data, and the questions this paper raises (who can see it, how long it is kept, and how it is audited) are the questions that plan exists to answer.

Va. Code § 22.1-20.2:1 addresses artificial intelligence systems used to support teaching, learning, assessment, or school operations, and calls for guidance on student data privacy and security in the context of those systems. Automated monitoring classifiers are machine-learning systems generating predictions about students. Guidance on how their outputs are reviewed and acted on fits squarely within that mandate.

The Department's existing Model Policy Concerning Internet Safety already addresses student privacy on school devices and safeguards for AI tools. A monitoring section would complete it.

B. Current Law Leaves the Key Questions Open

Va. Code § 22.1-289.01 governs vendor conduct: disclosure, privacy policies, access and correction, deletion on request, and a ban on selling student data. Federal laws (FERPA, COPPA, and CIPA) govern records, young children's data, and internet filtering. None of these sets limits on when monitoring may run, what content may be scanned, whether a person must review an automated flag, or when a flag may go to police.

C. Divisions Need a Common Standard

Division technology and legal staff are left to negotiate these questions vendor by vendor. A statewide standard reduces liability uncertainty, strengthens divisions' position in contract negotiations, and ensures that a student in one county has the same protections as a student in the next.

D. Other States Have Acted

Ohio enacted limits on school device monitoring in 2024. Ohio Revised Code § 3319.327 generally bars districts and vendors from monitoring location, audio and video features, and student interactions with school-issued devices, including keystrokes and web browsing, except under listed exceptions with written notice to parents. Virginia can adopt a more complete approach through Board guidance now and legislation later.

IV. Recommendations

1. **Adopt model guidelines on student activity monitoring.** The Board should adopt guidelines, modeled on Appendix A, addressing after-hours limits, prohibited features, human review, law enforcement referrals, retention, notice, and reporting.
2. **Update existing state guidance.** The Department should add a monitoring section to the model data security plan (§ 22.1-20.2), its AI guidance (§ 22.1-20.2:1), and the Model Policy Concerning Internet Safety, including retention limits for alerts and raw monitoring data and audit procedures for vendor access.
3. **Recommend standard vendor contract terms.** The Department should publish recommended contract provisions requiring vendors to disclose configuration options, disable after-hours scanning by default, document human review practices, report aggregate alert data, and certify deletion at contract end.
4. **Collect and publish statewide data.** The Department should ask divisions to report annual de-identified counts of alerts by category, alerts closed with no action, counseling referrals, disciplinary actions, and law enforcement referrals, and publish a statewide summary.
5. **Provide training guidance.** The Department should issue guidance on trained human review of automated alerts, emphasizing counseling-first responses and the principle that an automated flag alone is not reasonable suspicion.
6. **Support legislation.** The Board should support legislation in the 2027 Regular Session codifying these protections so they apply consistently across all divisions.

V. Anticipated Concerns

Concern	Response
Monitoring helps prevent suicide and violence	The guidelines preserve an emergency pathway and route flags to counselors first, with trained human review of context.
CIPA requires monitoring	CIPA requires filtering obscene or harmful images for E-Rate funding. It does not require scanning student writing or after-hours surveillance. The guidelines protect filtering.
This burdens divisions	Vendors already generate the configuration and alert data the guidelines ask divisions to report. A state standard reduces the work each division does alone.
Local control	The guidelines are a model that divisions adapt, consistent with how the Department supports divisions on data security today.

Appendix A: Proposed Model Guidelines

Model Guidelines for Student Activity Monitoring on School-Issued Devices and Accounts

1. Purpose. These guidelines assist school divisions in using student activity monitoring in a manner that protects student safety, privacy, and trust, consistent with Va. Code §§ 22.1-20.2, 22.1-20.2:1, and 22.1-289.01.

2. 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. 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.

3. Hours. Divisions should 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.

4. Prohibited features. Divisions should 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.

5. Human review. No automated alert should be the sole basis for discipline, a notation in a scholastic record, a parent notification disclosing sensitive personal information, or a law enforcement referral. A trained employee should review the full context first. An automated alert alone does not constitute reasonable suspicion.

6. Law enforcement referrals. Except in an emergency involving an imminent threat to life or safety, referrals based on monitoring should require written approval by the principal or designee and should be documented.

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

8. Retention. Alerts resulting in no action should be deleted within 90 days. Other monitoring data should be kept no longer than necessary, consistent with Library of Virginia retention schedules. Vendors should certify deletion at contract end.

9. Notice. Before issuing a device or account, and annually, divisions should give students and parents plain-language notice of each monitoring product, content monitored, hours of operation, alert recipients, referral policy, retention schedule, and complaint procedure.

10. Reporting. Divisions should publish and submit to the Department 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.

11. Contracts. Division contracts with monitoring vendors should require disclosure of configuration options, after-hours scanning disabled by default, documentation of vendor review practices, aggregate alert reporting, and certified deletion at contract end.

Sources

- Va. Code § 22.1-20.2, Student data security
- Va. Code § 22.1-20.2:1, Artificial intelligence system use and safety in instructional settings
- Virginia Department of Education, Model Policy Concerning Internet Safety
- 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)