

October 22, 2026

Chair Phil Mendelson
D.C. Council Committee of the Whole
1350 Pennsylvania Avenue, NW
Washington, DC 20004

EPIC's Public Testimony for D.C. Council Committee of the Whole Oversight Hearing on Technology in Schools

Dear Chair Mendelson and Members of the Committee:

Thank you for the opportunity to submit public testimony concerning technology in schools. This public testimony is submitted on behalf of the Electronic Privacy Information Center (EPIC).

EPIC is an independent nonprofit research organization in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has long advocated for student privacy by filing complaints, submitting public comments, filing amicus briefs, and pushing for comprehensive privacy legislation to protect students' privacy rights.

Over the years, EPIC has advocated for stronger procurement standards that improve the way governments acquire and use private-sector AI systems that impact residents' lives, including in education. For example, we have urged the Office of Management and Budget to adopt AI procurement guidelines that protect civil rights and increase transparency.¹ We have written about how states can protect privacy by closing the oversight gap on technology procurement.² We also published two relevant reports *Outsourced & Automated*,³ an in-depth look into state AI procurement, and *Assessing the Assessments*, a report that lays out the ideal elements of a risk assessment framework for automated decision-making systems.⁴

EPIC applauds the Committee's interest in understanding how schools are utilizing technology to educate students in the district and what impact this may have on students' learning

¹ EPIC et al., Comments Regarding the Office of Management and Budget's Request for Information on Responsible Procurement of Artificial Intelligence in Government (Apr. 20, 2024), <https://epic.org/wp-content/uploads/2024/04/Joint-Civil-Society-Comment-re-OMB-RFI-on-Responsible-Procurement-of-Artificial-Intelligence-in-Government.pdf>.

² Stephanie Forbes, *Protecting Privacy Through Stronger Procurement Policy: How Maine Could Pioneer a Better Approach to Technology Procurement*, EPIC (Sep. 3, 2026), <https://epic.org/protecting-privacy-through-stronger-procurement-policy-how-maine-could-pioneer-a-better-approach-to-technology-procurement/>.

³ Grant Fergusson, EPIC, *Outsourced & Automated: How AI Companies Have Taken Over Government Decision-Making* (2023), <https://epic.org/outsourced-automated/>.

⁴ Mayu Tobin-Miyaji, EPIC, *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risks Assessments* (2025), <https://epic.org/assessing-the-assessments/>.

and well-being. When used appropriately, some technologies can help advance educational goals. But weak procurement processes can enable harmful and unproven systems to come into schools, or can allow useful systems to be implemented in harmful ways.

EPIC’s testimony will primarily focus on educational technology (“edtech”) that utilizes AI or involves an automated system. Functionally, we consider an AI system to describe any system that automates a process, aids in human decision-making, or replaces human decision-making. While not all education technology incorporates AI, many learning tools have touted the benefits of AI and are used to aid or replace human decision-making. Similarly, schools have also adopted AI technology for school safety such as content monitoring services or weapons detection software.

EPIC encourages the Committee to consider students’ privacy rights when considering any legislation around the regulation of technology in schools. The Committee has the opportunity to intervene up front and improve public education governance by passing strong procurement guidelines that establish a process for auditing and verifying AI systems, incorporating protective contract language, developing oversight mechanisms, and set strong data privacy standards that protect students.

Student Privacy Must Be Protected in Matters Concerning Technology in Schools

Over the past few years, schools have adopted new edtech systems at a rapid rate, in part because edtech vendors have aggressively marketed supposed benefits of integrating AI into the learning process. These AI systems have been adopted for a variety of tasks such as school safety, test proctoring, grading, attendance monitoring, determining academic placement, and performance assessment. But without sufficient guardrails in place, these AI systems can materially impact students’ privacy, safety, civil rights, and academic outcomes in negative ways. Indeed, just this week, a bipartisan team of Senators wrote a letter to Google expressing concern about the effects of AI in schools and requiring Google to submit answers to important questions about its knowledge of harmful impacts on students.⁵

Edtech tools have been a privacy and cybersecurity nightmare for students. Edtech vendors have used the guise of education to collect and commodify student’s personal data for purposes that are unrelated, even out of context, of the educational mission. For example, edtech vendors have collected children’s personal information to behaviorally profile them for advertising purposes and to feed into training data for other predictive analytics products.⁶ PowerSchool Naviance, an edtech vendor, settled a case alleging that it harvested students’ private communications and data to sell to

⁵ Letter from Senators Blumenthal and Hawley to Google Concerning AI Impacts in Schools (Oct. 21, 2026), https://www.blumenthal.senate.gov/imo/media/doc/letter_to_google_re_ai_tools_impacting_studentspdf.pdf.

⁶ See e.g., Press Release, FTC, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children’s Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising>; Todd Feathers, *This Privacy Equity Firm Is Amassing Companies that Collect Data on America’s Children*, The Markup (Jan. 11, 2022), <https://themarkup.org/machine-learning/2022/01/11/this-private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children>.

data brokers.⁷ The student data can also be a target for bad actors, and edtech vendors are not immune from data breaches. For example, PowerSchool experienced a breach that allowed hackers to steal personal data of students and teachers.⁸ PowerSchool eventually paid these hackers an undisclosed sum to not release the stolen data that may have included sensitive information like Social Security numbers, names and addresses, grades, and medical information.⁹ Similarly, the FTC recently finalized a settlement order with Illuminate Education Inc. after finding that the edtech company failed to protect the privacy and security of student data that resulted in a data breach exposing 10.1 million students' personal information.¹⁰

AI edtech tools can pose a particular threat to students' civil rights, especially for students from historically marginalized communities. AI technologies reproduce the outcomes represented by the training data on which they are built, so systems based on biased historical training data will reproduce that bias and have disparate impacts on students of color, women, and others.¹¹ These biased outcomes are especially concerning in important or high-risk contexts such as in school safety surveillance, predictive analytics for student behavior, or grading and assessment. Moreover, AI surveillance technologies are often concentrated in schools with predominantly poor and minority students.¹²

Another issue with AI-enabled edtech is mission creep that violates students' privacy and safety. In one use case, schools have been adopting AI technology to monitor student online activity on school provided devices. From monitoring for violation of school policies, use cases have expanded their mission to other issues like monitoring for threats of suicide and self-harm. While it is not necessarily bad to monitor for those outcomes, such monitoring must be performed carefully and thoughtfully—presumably, at the behest of schools through procurement guidelines that lay out a well-reasoned process. That does not seem to have been the case. Companies such as Lightspeed, which has a contract with D.C. Public Schools (“DCPS”), use AI tools to identify possible risks and notify not only the school to possible self-harm, but also law enforcement officers.¹³ Similar tools

⁷ See Christopher Brown, *Powerschool to Pay \$17.25 Million to Settle Student-Data Suit*, Bloomberg Law (Feb. 24, 2026), <https://news.bloomberglaw.com/litigation/powerschool-to-pay-17-25-million-to-settle-student-data-suit>.

⁸ Carly Page, *Edtech Giant PowerSchool Says Hackers Accessed Personal Data of Students and Teachers*, TechCrunch (Jan. 8, 2025), <https://techcrunch.com/2025/01/08/edtech-giant-powerschool-says-hackers-accessed-personal-data-of-students-and-teachers/>.

⁹ *Id.*

¹⁰ Press Release, FTC, FTC Gives Final Approval to Order Against Illuminate Settling Allegations It Failed to Secure Students' Personal Data (June 5, 2026), <https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-gives-final-approval-order-against-illuminate-settling-allegations-it-failed-secure-students>.

¹¹ Christine Chambers Goodman, *Disparate Impacts of Algorithmic Bias on Primary and Secondary Educational Opportunities*, in *Understanding and Addressing Digital Inequalities* (Danielle Borges et al. eds., 2026), <https://ssrn.com/abstract=7589863>.

¹² Sidra Sheikh, Alexis Stolberg, & Allison F. Gilmour, *Investigating Advanced School Surveillance Practices and Disproportionality: A Systematic Review*, 60 Urb. Educ. 2438 (2025), <https://journals.sagepub.com/doi/10.1177/00420859241279446>.

¹³ Lightspeed Systems, *Lightspeed Filter* (2026), <https://www.lightspeedsystems.com/products/lightspeed-filter/>.

have also flagged, however, sensitive private activity, such as whether a student is LGBTQ+. ¹⁴ This is inappropriate and even dangerous for students, such as when alerts are shared with U.S. Immigration and Customs Enforcement. ¹⁵ False, or even true, alerts can lead to extremely traumatic interactions with law enforcement for students and make students feel less safe.

Another issue is AI systems' inaccuracy when deployed to identify people of color. For years, schools have adopted facial recognition systems to alert school personnel and law enforcement when a "person of interest" enters the campus. ¹⁶ However, facial recognition software is more likely to misidentify people of color and women, which can lead to false matches. ¹⁷ More recently, schools have partnered with companies that offer license plate readers and predictive behavior modeling all in the name of student safety, though there is a growing movement from many districts to reexamine their contracts with companies like Flock. ¹⁸ Schools have also implemented the use of algorithms to detect weapons, vape, or other prohibited items, ¹⁹ many of which display severe accuracy problems and concerning levels of mission creep. ²⁰

The Committee Can Address Risks Posed by Edtech and AI Systems By Passing Meaningful Procurement Guardrails

To mitigate the risks posed by AI and automated decision-making systems, the Committee should pass legislation that establishes strong procurement standards for schools. Often, it is weak procurement processes that allow harmful and or unproven technology to enter schools. Strong procurement standards can effectively regulate edtech by protecting student data, ensuring safety and

¹⁴ Claire Bryan & Sharon Lurye, *Schools Use AI to Monitor Kids, Hoping to Prevent Violence. Our Investigation Found Security Risks*, Assoc. Press (Mar. 12, 2025), <https://apnews.com/article/ai-school-chromebook-gaggle-goguardian-securlly-25a3946727397951fd42324139aaf70f>.

¹⁵ See e.g., Joseph Cox, 'Bus Patrol' Put AI Cameras in Tens of Thousands of School Buses. Now They Want to Give Cops Access, 404 Media (May 26, 2026); Mark Keierleber, *ICE Taps Into School Security Cameras to Aid Trump's Immigration Crackdown, 74 Investigation Finds*, The 74 (Feb. 10, 2026), <https://www.the74million.org/article/ice-taps-into-school-security-cameras-to-aid-trumps-immigration-crackdown-74-investigation-shows/>.

¹⁶ See Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, N.Y. Times (Feb. 6, 2020), <https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html>.

¹⁷ Marcus Smith & Monique Mann, *Facial Recognition Technology & Potential for Bias and Discrimination*, *The Cambridge Handbook of Facial Recognition in the Modern State* 87, 91 (Rita Matulionyte & Monika Zalnierute, eds., 2024), <https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technology-and-potential-for-bias-and-discrimination/AD79286EF1A571682F3D86238F6AB467>.

¹⁸ See e.g., Maggie More & Drew Wilder, *Fairfax County School Board Bans All Flock-Style Cameras on School Property*, NBC Washington (Sep. 25, 2026), <https://www.nbcwashington.com/news/local/fairfax-county-school-board-bans-all-flock-style-cameras-on-school-property/4159270/>.

¹⁹ Ashlyn Campbell, *MCPS is Piloting an AI-Based Safety System. What Will it Look Like?*, Bethesda Magazine (Feb. 12, 2026), <https://bethesdamagazine.com/2026/02/12/mcps-ai-safety-system/>; Todd Witney, et. al, *Unproven Vape Detection Tech Expands Surveillance in Schools, Threatening Privacy*, Tech Policy Press (Oct. 16, 2025), <https://www.techpolicy.press/unproven-vape-detection-tech-expands-surveillance-in-schools-threatening-privacy>.

²⁰ Katie Barlow, *High School Vape Sensors Trigger "Thousands" of False Alarms at MCPS Schools*, FOX 5 DC (Sept. 17, 2025), <https://www.fox5dc.com/news/high-school-vape-sensors-trigger-thousands-false-alarms-mcps-schools>.

vendor compliance, and eliminating bias. Support from the Committee in establishing these guardrails can create also create strong enforcement standards and ensure that DCPS is not policing their own compliance and contract enforcement.

Many state and local governments, including D.C., use the same procurement processes for purchasing edtech as they do for simpler goods and services. Edtech vendors should not be held to the same standard as vendors for office supplies. D.C.'s current procurement processes do not support the oversight and accountability needed to manage the growing risks that edtech systems can pose. There is no clear structured review that includes the necessary level of risk analysis needed. Edtech vendors claim to be innovative and aggressively market themselves to schools to adopt their systems quickly. Edtech vendors often promise accurate, fair, and effective systems but many fall short to its claims. Schools and impacted students often have no recourse when a vendor falls short of their promises or worse, experience harmful outcomes from the technology or from security breaches.

While EPIC recommends government wide procurement standards that can have the greatest impact across sectors, focusing on school specific procurement standards is a positive step forward for the Committee. There is a plethora of recommendations for procurement frameworks that the Committee could model legislation after, including those found in our referenced reports.

Below we have included some recommendations on establishing a strong procurement standard, advise the Committee to restrict harmful high-risk use cases, and urge the Committee to increase transparency and recourse for impacted students.

Procurement Standard Recommendations

The Committee should initially establish benchmarks on safety, privacy, data security, and equity that need to be met before vendors are eligible to sell their technology to schools. The Committee should also establish a consistent set of obligations for edtech vendors when it comes to their data privacy practices. By adopting specific, standardized contract clauses, schools can proactively protect students before harms occur. At minimum, data privacy agreements should include the following:

- **Data minimization:** data collection should be limited to what is strictly necessary to accomplish the purpose set out in the contract; data should be deleted in a short time period after its use is no longer necessary for the originally intended purpose.
- **Purpose limitation:** any use or transfer of personal data should be limited to what is reasonably necessary for the intended purpose as defined by the school.
- **Data ownership:** the District should retain ownership and exclusive control of any data collected by edtech systems, any sale or transfer of personal or sensitive data to unauthorized third parties must be prohibited.
- **Adequate cybersecurity protection:** vendors must abide by the District and federally required cybersecurity standards and comply with applicable data breach laws.
- **Risk and impact assessments:** require independently conducted impact and risk assessments for AI systems, especially high-risk AI systems.

- **Independent audits:** require independently prepared audits that review the data used to train an operate an AI system, stress testing of the AI system under different situations, and regular testing to ensure fairness and accuracy of the system's outputs.
- **Effectiveness and accuracy verification:** vendors must prove that their technology is effective as advertised in the procurement and marketing materials and serves the purpose laid out by the school.
- **Termination procedures:** if a vendor is found to be in breach of contract, the school should reserve the right to terminate the agreement and request immediate deletion of all data collected.
- **Other protective language:** contractual language should focus on improving data oversight and control, imposing transparency or reporting requirements, incorporating sunseting clauses or procedures to transition ownership, and requiring human review for automated decision-making results.

As part of the procurement process, the Committee should establish a risk assessment framework that forces vendors to carefully evaluate and disclose the risks associated with any AI, automated decision-making, and planned data processing. Conducting risk assessments supports thoughtful adoption of technology and understanding of risk mitigation procedures as well as increase transparency prior to adoption.

An ideal risk assessment framework includes:

- **Enforceable legal obligations:** edtech vendors should not self-police their practices, the Committee should adopt a legal framework that requires risk assessments prior to procurement.
- **Clear thresholds:** for robust privacy protection, the Committee should set low minimum thresholds for when a risk assessment must be conducted. EPIC recommends, at minimum, the threshold to include any collection or process of sensitive personal data and any use of AI or automated decision-making systems.
- **Transparency and public access:** the public should have access to risk assessments in a centralized, easily searchable database and disclosed to people in a conspicuous, accessible manner.
- **Clear and thorough content requirements:** for a robust list of information that should be included in a risk assessment see our *Assessing the Assessment Report*.²¹
- **Have specified methods for measuring privacy impacts:** the Committee, in consultation with education experts and other stakeholders, should develop detailed privacy harms and human rights guidance for an edtech vendor to assess.
- **Independent assessors:** require that assessments be conducted by a third-party. Independent assessors that are credible or certified with no financial interest in the outcome of the risk assessment are more likely to conduct an objective assessment.

²¹ Tobin-Miyaji, *supra* note 4, at 34–38.

Restricting High-Risk AI Uses Cases

EPIC has long advocated for the restriction of high-risk harmful AI uses. Risk of harm from AI systems often depends on when and how systems are used as well as whether they are appropriate and necessary for the intended educational purpose. High-risk AI systems where harms cannot be sufficiently mitigated should not be used. In the beginning of the procurement process, schools can utilize audits and assessments to get enough information to identify risks and determine when they should stop or prevent the use of AI systems. Audits also come into play during the contracting period where schools can include contractual provisions that require ongoing testing or evaluation throughout the course of the contract for high-risk systems.

Increasing Transparency and Recourse for Impacted Students

The procurement process should include transparency mechanisms that allow students and other members of the community to thoughtfully participate in the adoption of AI systems in schools. Transparency requirements can be carefully crafted to navigate around any trade secret and property right challenges while still providing enough information for schools and the public to perform procurement due diligence. The Committee should also require that DCPS complete and publicly post impact assessments and provide opportunity for community feedback prior to deployment as well as establish a publicly accessible and regularly updated edtech inventory. Greater transparency mechanisms also allow for greater public oversight and accountability for both DCPS, the Committee, and edtech vendors.

The Committee should also mandate strong transparency requirements to improve the public's awareness and parents'/student's rights around technology use in schools and provide redress mechanisms for when students have been harmed. It is often difficult for families to know if their student has been harmed by an edtech tool. They are not always notified when they were subject to an automated decision-making system, or a flawed assessment determined an educational outcome that has consequential impacts in the future. It is also difficult to challenge incorrect decisions from AI or automated decision-making systems. Families and students need access to robust notices and opportunities to appeal or opt out of AI decisions. To empower those impacted by these systems, there could be contractual provisions that grant "third-party beneficiary rights" where students can pursue a contractual remedy either in court or directly with the school or vendor.

Conclusion

Technology can be utilized thoughtfully and in limited use cases to support educational goals. But there are also real privacy risks involved in deploying unproven edtech. The Committee should be the example for DCPS, the D.C. State Board of Education, and the D.C. Public Charter School Board and it can do so by centering student privacy in regulating technology in schools. We urge the Committee to pass meaningful procurement guidelines that set the condition for how technology is purchased and deployed in schools—before harmful practices are entrenched. Having robust procurement standards for edtech can tackle many of the issues raised by community members in this hearing.

EPIC also strongly encourages the Committee to pass legislation that incorporates thoughtful technology adoption practices for all technology, not just edtech, that can have significant impacts

on privacy, safety, civil rights, and disciplinary or educational outcomes. Procurement guardrails is a sensible approach to the government adoption of technology and can have significant positive impacts for everyone in the District.

Thank you for the opportunity to submit testimony on this important topic. EPIC is happy to serve as a resource to the Committee on these issues.

Respectfully submitted,

/s/ Enid Zhou

Enid Zhou

EPIC Senior Counsel

/s/ Tom McBrien

Tom McBrien

EPIC Counsel