LEGAL MAILBAG – FEBRUARY 19, 2026

By Attorney Joseph Miller, Associate, Shipman & Goodwin LLP – GUEST COLUMNIST

The "Legal Mailbag Question of the Week" is a regular feature of the CAS Weekly NewsBlast. We invite readers to submit short, law-related questions of practical concern to school administrators. Each week, we will select a question and publish an answer. While these answers cannot be considered formal legal advice, they may be of help to you and your colleagues. We may edit your questions, and we will not identify the authors.
Please submit your questions to: legalmailbag@casciac.org.

Dear Legal Mailbag,

Your posts are so helpful to us school administrators—we appreciate you!

The latest misbehavior we've been facing from high-schoolers is sprouting from the AI world. Students can copy a picture posted to a peer's social media and run it through an app that manipulates the photo in ways that can be anywhere from unflattering to graphic. Knowing that the sharing of such content is cyberbullying and can be potentially illegal, we try to investigate these reports and hold students properly accountable.

My question is related to student searches: what are my legal rights if I'm suspicious that a student's cell phone might contain AI-doctored photos or videos of a peer? If the alleged offender refuses to unlock their phone or show me the camera roll, do I just assume they possess the content in question? Also, how does the age of the victim and the nature of the content impact my actions in such searches?

Signed,
What's Real These Days?

Dear What's:

You've raised a timely question. Although artificial intelligence (AI) has the capacity to improve teaching and learning in a multitude of ways, Legal Mailbag takes no pleasure in observing that its potential for misuse in the educational setting is similarly vast. When students deploy these powerful tools to humiliate or demean others, the implications for the perpetrator and the victim alike can be far-reaching and serious.

This is not an isolated problem. A recent national survey by RAND Homeland Security Research Division found that 13 percent of K-12 principals reported incidents of bullying that involved AI-generated "deep fakes" during the 2023-2024 and 2024-2025 school years. That number rose to 20 percent for middle school principals and 22 percent for high school principals.

Naturally, you'd like to head off these issues before they occur in your building. Laudable as these efforts may be, it is essential that you keep in mind the constitutional protections to which your students are entitled—even those you are convinced are harboring deep fakes of *you*.

As you no doubt are aware, the Fourth Amendment protects individuals from "unreasonable searches and seizures" by the government, and school officials are considered to be government agents. Courts and legislatures (not to mention boards of education and administrators) have long struggled to balance students' expectation of privacy with school authorities' interest in maintaining safety and order.

The seminal case that governs when a student or their possessions may be searched is *New Jersey v. T.L.O.*, 469 U.S. 325 (1985). In that case, the United States Supreme Court established a two-part test for determining whether a search conducted by school officials is reasonable. First, the search must be "justified at its inception"—there must be a reasonable basis, *before* the search is conducted, to suspect that it will uncover evidence that a student has violated the law or school rules. Second, the search must be "reasonably related in scope" to the reason for the search and must not be excessively intrusive in light of the student's age, sex, and the nature of the alleged infraction.

Technological advances often outpace the laws that regulate their use. Although AI was still the stuff of science fiction when *T.L.O.* was decided, it remains the standard for assessing the reasonableness of a student search.

What constitutes a "reasonable basis" for searching a student's cell phone? A school official's suspicion of wrongdoing must be based on specific and articulable facts, not a hunch or a guess. Often, that means a credible report from a staff member, student, or parent, or an observation of behavior that suggests that a search will yield evidence of rule-breaking. In other words, it is not enough that an administrator is generally aware that illicit AI-generated content is being circulated. There must be a factual basis to suspect that a search of a particular student's phone will produce evidence of the misconduct.

Administrators should not assume that, simply because they are justified in *confiscating* a student's phone, they are likewise entitled to search it. Courts in different jurisdictions have reached inconsistent conclusions with respect to whether the violation of a school rule prohibiting the possession or use of a cell phone is sufficient cause for a search. Legal Mailbag counsels that you will need to point to specific facts that give rise to a belief that a search will yield evidence of a violation of law or of school rules.

If there are legitimate grounds for a search, it must be narrowly tailored to the facts that justified it. The Supreme Court has noted, albeit in a different context, that searches involving cell phones pose heightened privacy concerns because today's phones contain vast amounts of personal information. *See Riley v. California*, 573 U.S. 373 (2014). Accordingly, when a student's phone is searched for inappropriate AI-generated content, the search should be limited to the areas of the phone where such content is likely to be stored—a social media or messaging platform, for instance, or an AI app that records the history of its output.

Administrators can protect themselves from prospective Fourth Amendment claims by following some straightforward best practices. Always ensure that there is a reasonable factual basis for searching a student's phone. Restrict the search to locations that, based on those facts, are likely to contain evidence of misconduct. As curious as you may be, do not browse or download unrelated personal information.

If a student refuses to submit to a phone search, Legal Mailbag would not advise you to consider that, in itself, to be tantamount to a confession. However, if you have satisfied the constitutional bases for a search, you may consider the student's refusal to consent to a search to be insubordination. You may certainly weigh that fact accordingly as you investigate the alleged misconduct consistent with the applicable school climate and discipline policies.

Legal Mailbag offers one additional thought for consideration. Though some AI-generated content used in cyberbullying may be "merely" hurtful or distasteful, it is illegal to publish or share nonconsensual intimate imagery, including that which is created by AI. And if the sexually explicit content depicts a person under the age of sixteen, it may constitute child sex abuse material, the definition of which under Connecticut law specifically includes computer-generated images or pictures and the possession of which can be a felony. *See* Conn. Gen. Stat. §§ 53a-193(13), 53a-196d *et seq*. Reminding students of these facts may help to reinforce that such misuse of AI is no laughing matter and may well have serious consequences.