KEEPER®

AI in Schools Report
Balancing Adoption With Risk

October 2025

Overview

Artificial Intelligence (AI) is transforming education. Teachers are using it to plan lessons, draft communications and analyze student performance. Students are turning to AI for research, brainstorming and creative projects. Across classrooms, the technology is freeing up time and creating new opportunities for learning.

Yet, adoption is outpacing preparedness. Forty-one percent of schools report they have already experienced AI-related cyber incidents, ranging from phishing campaigns to harmful student-generated content. While awareness of risks is high, policies remain inconsistent and confidence in recognizing threats varies widely.

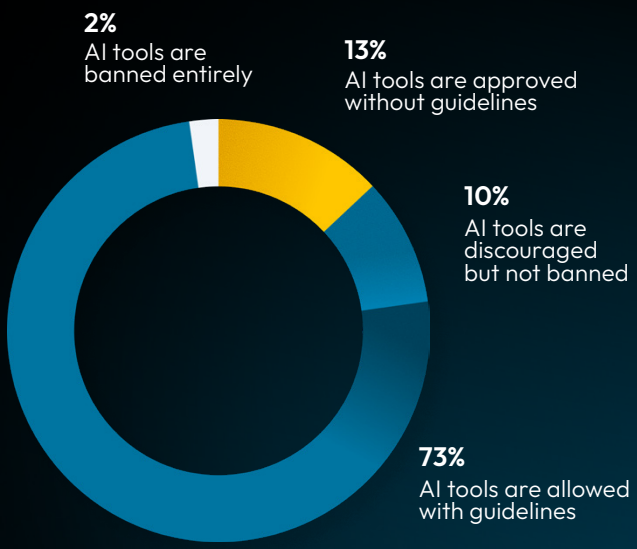
This report, based on a survey of more than 1,400 education leaders across primary, secondary and higher education in the United States and the United Kingdom, examines how AI is being used in schools today, where safeguards have been implemented, where gaps remain and what steps institutions can take to ensure AI strengthens education, rather than disrupts it.

AI Is the Norm in Classrooms and Faculty Offices

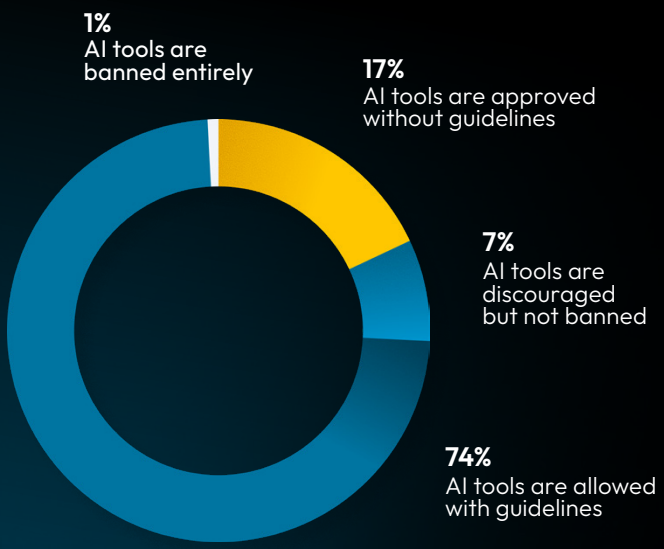
AI is now a common part of classrooms and faculty offices. Eighty-six percent of institutions permit students to use AI tools, while only 2% have banned them outright. Among faculty, adoption is even higher at 91%, often with guidelines in place.

Students are primarily using AI for supportive and exploratory tasks. The most common uses are research (62%), brainstorming (60%) and language assistance (49%). Creative projects (45%) and revision support (40%) follow, while more sensitive uses like coding (30%) and completing assignments (27%) are more tightly controlled.

What is your institution's current stance on AI tool usage by students?



What is your institution's current stance on AI tool usage by faculty and staff?

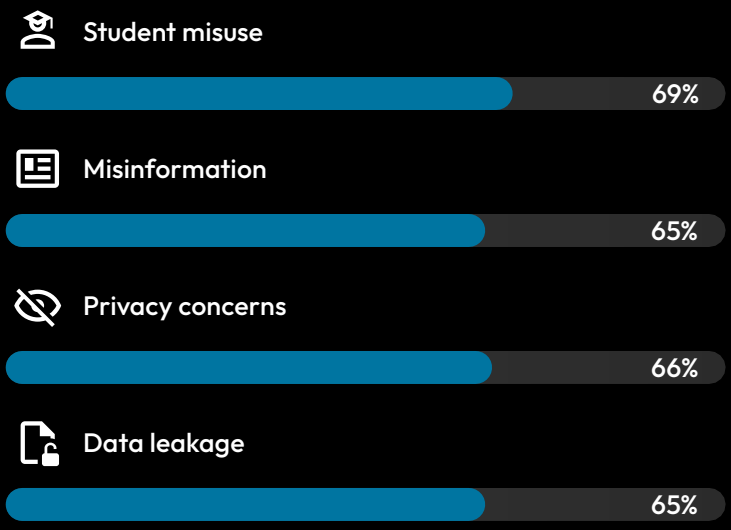


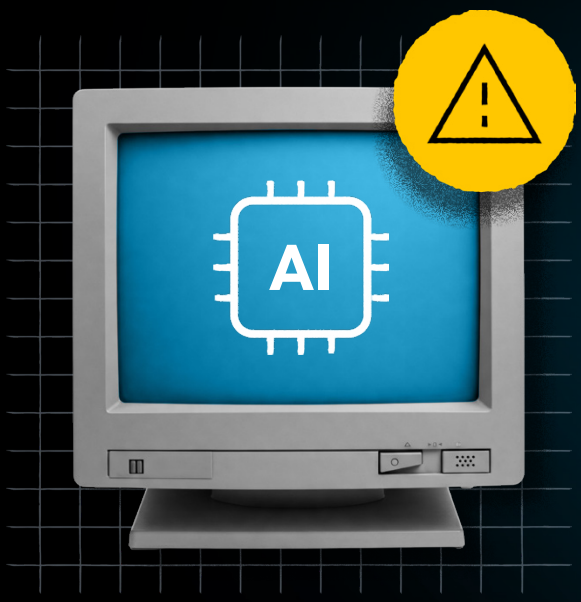
Faculty adoption is driven by efficiency. Administrative functions such as scheduling (67%) and lesson preparation (60%) are the primary uses. About half of institutions allow staff to use AI for grading, student engagement strategies and data analysis.

This data shows a clear divide: schools are encouraging staff to use AI to improve productivity, while limiting student use to exploratory activities to maintain academic integrity.

Mixed Confidence Levels in Recognizing AI Threats

Which AI cybersecurity risks are you aware of?

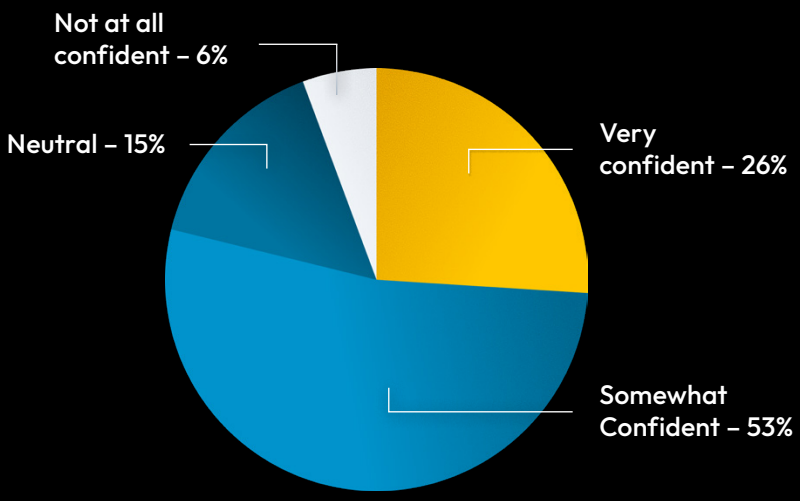




Awareness of potential AI-related cybersecurity risks is reassuringly high (83%), but the depth of understanding is uneven.

While many say they recognize common risks associated with AI use, like data leakage, privacy concerns and the potential spread of misinformation, fewer are aware of more technical or emerging threats. According to Keeper Security's 2025 Future of Defense report, 95% of IT leaders reported cyber attacks are more sophisticated than ever – and they are unprepared for this new wave of threat vectors.

How confident are you in recognizing AI-related cyber threats (e.g., deepfakes, AI-powered phishing)?

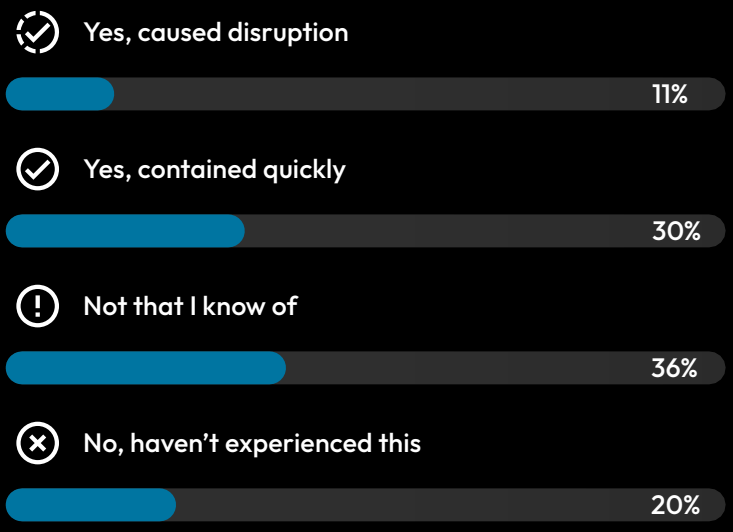


Most educators think they can spot an AI scam, but only one in four feels truly confident. With 41% of schools already reporting AI-related cyber incidents, that gap could leave schools exposed.

The combination of broad awareness with limited technical readiness requires a multi-layered approach: combine employee training and awareness with data encryption, advanced threat detection and access controls (including password managers and PAM) to prevent AI-powered attacks and reduce the blast radius when incidents occur.

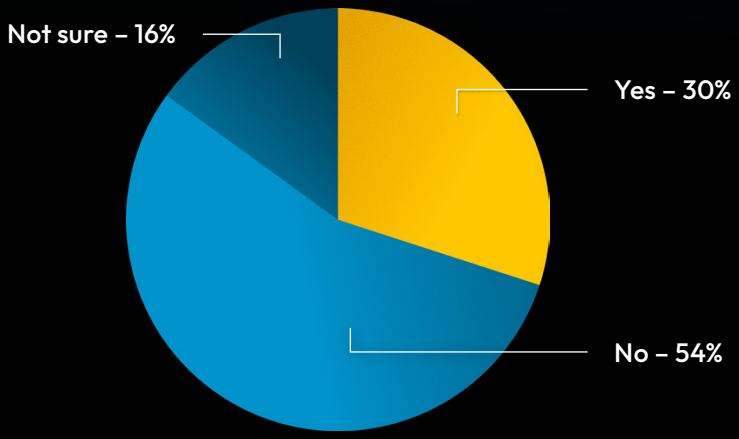
AI-Related Incidents Are Happening in Schools

Has your institution been targeted by any AI-generated phishing attempts or misinformation campaigns (e.g., deepfake videos, synthetic audio)?

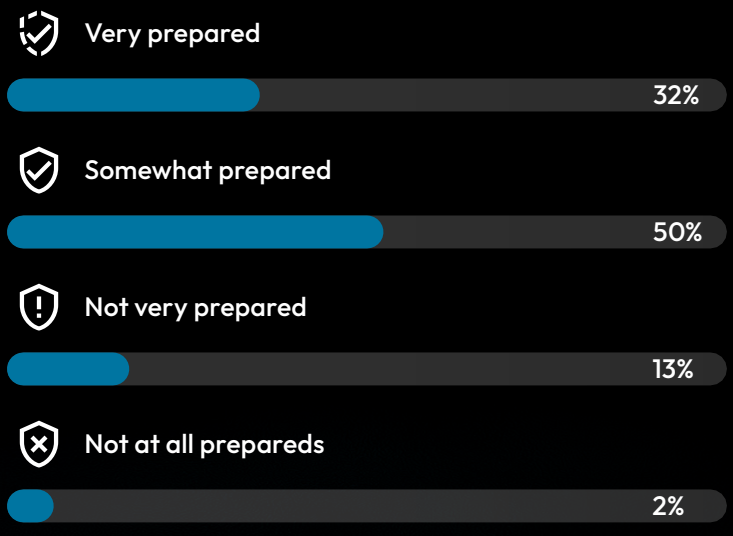


Schools are already experiencing AI-related incidents, both internally and externally. Forty-one percent said they have faced phishing, misinformation and other disruptive efforts, while nearly 30% reported instances of students producing harmful AI content. While most confirmed events were "contained quickly" (30%), a majority of respondents (39%) were unsure whether incidents had occurred, suggesting sizable gaps in monitoring and awareness.

Has your school experienced students creating harmful AI content (deepfakes of peers, etc.)?



How prepared is your institution to handle AI-related cybersecurity threats over the next 1–2 years?



Most institutions (82%) said they feel at least “somewhat prepared” to handle AI-related cybersecurity threats, though that number falls to 32% for those who feel “very prepared.” This confidence, tempered by caution, aligns with earlier themes: schools are aware of risks, but sizable gaps remain in overall preparedness and uncertainty persists about the effectiveness of existing safeguards.

The Cybersecurity Concerns

Overall concern about AI-related cybersecurity threats:

37%
Very concerned

53%
Somewhat concerned

10%
Not concerned

What are you most concerned about?

65%
Student privacy violations

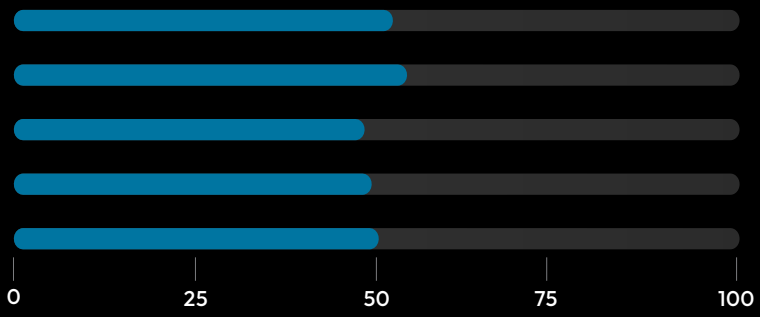
53%
Learning disruption

52%
Deepfake impersonation of staff/students

With more than 40% already impacted, concern among faculty around AI-related cybersecurity threats is, unsurprisingly, almost universal, with 90% of respondents at least “somewhat concerned.” More than a third (37%) said they were “very concerned,” with student safety and learning outcomes - including privacy violations, deepfake impersonation and potential learning disruption - topping the list of anxieties. There is also substantial worry about bias in AI outputs (43%), reputational harm (37%) and financial damage (36%), risks that threaten both operational and reputational resilience.

Policies and Safeguards are Fragmented

How is your school or university addressing AI-generated phishing and misinformation?*



- 51% Detailed policies/guidance
- 53% General awareness/informal guidance
- 47% Updating or developing policies
- 48% Staff training on detecting phishing/deepfakes
- 49% Student education on misinformation/disinformation

While schools and universities are building frameworks to govern AI use, implementation is uneven. Policy development is still playing catch-up to practice: just over half have detailed policies (51%) or informal guidance (53%) in place, while less than 60% deploy AI detection tools and student education programs. With more than 40% already impacted, the fact that only a third (34%) have dedicated budgets and just 37% have incident response plans indicates a concerning gap in preparedness. Privacy, consent and educational purpose guidelines lead the way in terms of active policies. The vast majority of schools (90%) already have policies or expect them within six months to a year, although the number drops to 42% for those that currently have a policy in place.

Perceptions of the reliability of AI detection tools are moderate at best: just 26% see them as being “very reliable” in their current form, highlighting the limitations of technical safeguards alone. Faculty training is split between formal (37%), peer-based (36%) and informal (19%) approaches, suggesting institutions are still experimenting with the best ways to build AI literacy and cybersecurity awareness.

***Additional statistics**

Technical tools: 20%
Collaboration with external cybersecurity partners: 19%
Not currently taking steps: 3%

The Road Ahead: Closing the Gap Between Adoption and Readiness

The question today is not whether to adopt AI, but how to govern, secure and guide its use while controlling existing and emerging threats. This report shows that institutions are already falling behind in effective policy, governance and budgeting compared with the speed of AI adoption. This lag in governance, training and updated security measures may prove even more detrimental in the immediate future, as institutions already report facing AI-driven threats and harmful misuse.

The data suggests three key imperatives for education leaders today:

- **Close the policy gap:** Formalize AI policies that balance adoption with responsible use.
- **Strengthen resilience:** Invest in training, awareness, cybersecurity and detection tools to better prepare staff and students for AI-enabled threats.
- **Safeguard trust:** Address privacy and ethical concerns directly, ensuring measures to manage AI use do not erode student or community confidence.

In practice, this means taking immediate, actionable steps to strengthen defenses:

- Enforce Multi-Factor Authentication (MFA) across all systems to reduce the risk of compromised accounts.
- Adopt a Privileged Access Management (PAM) solution to control who can access sensitive data and critical systems.
- Teach strong password practices to staff and students to reduce one of the most common entry points for attackers.
- Deploy real-time detection and monitoring to spot AI-enabled phishing, deepfakes and other new threats before they escalate.
- Regularly review and update AI policies to ensure they keep up with new technologies, risks and use cases in the classroom.

For schools and universities, the next two years will be crucial in deciding whether AI becomes a trusted partner in education or an ongoing vulnerability. Taking these proactive steps now can help institutions keep pace with adoption while staying ahead of the evolving threat landscape.

Methodology

Keeper Security, a cybersecurity innovator and provider of the leading zero-trust and zero-knowledge Privileged Access Management (PAM) platform, commissioned independent research agency TrendCandy to survey 1,460 education administrators in the US and UK about how schools are navigating AI adoption, usage and cybersecurity readiness.

The online, compensated survey was targeted to key leaders at educational institutions across the US and UK in accordance with stringent survey methodology requirements including randomized sampling, double-blind practices and data-quality controls.

The margin of error for this study is +/- 3% at the 95% confidence level.

About Keeper Security

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access, endpoint privilege management and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organization against today's cyber threats at KeeperSecurity.com.