FACT SHEET

Navigating the AI Frontier in K-12 Cybersecurity for District Administrators

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS TECHNICAL ASSISTANCE CENTER

Artificial intelligence (AI) has a decades long history in K-12 education, evolving from early Intelligent Tutoring Systems to adaptive intelligence driven by machine learning and Natural Language Processing. Today, AI continues to transform K-12 education by advancing personalized learning, automating administrative tasks, enhancing analytics, and supporting diverse learners. This progression has increased cybersecurity risks, including the appropriation of sensitive student data. This fact sheet provides K-12 leaders with insights for protecting student data and ensuring operational resilience in an AI-driven world. K-12 leaders can use this information to inform the development and enhancement of school emergency operations plans (EOPs).

AI's Influence on Cybersecurity

AI offers education agencies unique opportunities and risks. While it provides advanced tools for instruction and technological support, it also empowers malicious actors.

AI as an Enabler

- **For Malicious Actors**: AI lowers the barrier to entry for cybercriminals, enabling them to craft highly convincing phishing emails, develop tailored attacks, create deepfakes for social engineering, and automate exploitation.
- **Shrinking Patching Window**: AI accelerates the discovery and exploitation of vulnerabilities, drastically reducing the time available for information technology teams to apply critical security patches.
- **For Cyber Defenders**: AI enhances threat detection, predictive analytics, and automated incident response. It also reduces alert fatigue.

Key AI and Cybersecurity Terms

Generative AI (GenAI) is AI that generates new content from trained data.

Large Language Model is an AI model trained on vast amounts of text data.

Phishing is a social engineering attack often used to steal user data.

Deepfake is synthetic media copying or modifying a person's likeness.

AI as an Amplifier Within the K-12 System

AI magnifies both positive and negative aspects within a K-12 district's technological environment. Existing weaknesses, errors, or vulnerabilities can have significant and widespread consequences.

- **Amplifying Mistakes and Errors**: AI systems can amplify the impact of human errors, data inaccuracies, or system misconfigurations.
- **Amplifying Data Breaches**: Data breaches in AI-enabled environments can lead to the compromise of a larger volume and variety of sensitive data. As an example, an AI-powered surveillance tool intended to monitor student communications for safety threats like self-harm or bullying inadvertently led to the exposure of nearly 3,500 unredacted student documents. These documents contained highly sensitive personal information, including essays, diaries, and mental health discussions.
- **Amplifying Positive Impacts:** AI can enhance personalized learning and administrative efficiency.

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS REMS TECHNICAL ASSISTANCE CENTER

FOR MORE INFORMATION

(855) 781-REMS (7367) info@remstacenter.org @remstacenter https://rems.ed.gov

AI as a Permanent Data Repository

AI systems often embed training data irreversibly, which poses significant implications for data governance and student privacy regulations like the *Family Educational Rights and Privacy Act* (FERPA). In many cases, data cannot be corrected, modified, or deleted without deleting the entire AI model.

AI Confidentiality Concerns

AI-powered search and assistant tools can surface overshared or improperly permissioned data within cloud environments, leading to unintentional exposure of sensitive information.

Tactical Considerations for K-12 Operations

The integration of AI necessitates a fundamental re-evaluation of cybersecurity practices, data management, and incident response.

- **Rethinking Incident Response Times**: The speed of AI-driven threats demands faster response times and the integration of automated mechanisms. Additionally, critical internet-exposed vulnerabilities need to be patched in days, not weeks.
- **Limiting Data Uploads and Practicing Data Minimization**: A paradigm of data minimization is essential to limit the amount and sensitivity of data provided to AI systems and use masking or proxy options where available.

How to Mask and Proxy Data

When you're feeding data to public AI, masking and proxying are essential.

Masking means altering or hiding sensitive details in your data—think swapping real names for fake ones or partially obscuring account numbers. The goal is to make the data unidentifiable but still useful for the AI.

Proxying involves using a middleman. Instead of sending your data directly, a proxy acts as an intermediary, replacing or substituting identifying information like student ID numbers before it reaches the AI.

Both methods protect your privacy and sensitive data, letting you leverage AI with less risk of exposure or non-compliance.

- **Strengthening Data Governance for AI**: Safe AI adoption requires robust data governance, including policies on data classification, access controls, and lifecycle management.
- **Managing Procurement and Vendor Tools**: Procurement processes must include rigorous AI-specific security, privacy, and ethical vetting. Access permissions for vendor and API tools also need to be reviewed and limited.
- **Enhancing Cybersecurity Training and AI Literacy**: All stakeholders require training on the responsible use of AI and its data privacy implications.

Sample Questions for Vetting AI Educational Technology Vendors

- What specific student data and metadata does your AI tool collect?
- Is student personally identified information used to train your AI models, and if so, is it anonymized or de-identified?
- How do you ensure FERPA compliance in terms of parent access and corrections?
- What are your data retention policies, and do you offer "machine unlearning" capabilities?
- What training and support do you provide for educators?

History of AI in Education: From Origins to Future. 2025. *The School House Anywhere.*

PLEASE NOTE: The tools and resources identified in this document are not intended as endorsements and are merely offered as examples that you may consider in your own planning efforts.

Strategic Recommendations for K-12 Executives

To comprehensively update and implement AI-informed EOPs, K-12 leaders should explore ways to:

- **Champion a Culture of AI Security Awareness**: Foster ongoing AI literacy and cybersecurity training for all stakeholders.
- **Adopt a Risk-Based Approach to AI Implementation**: Conduct risk assessments for new AI systems and pilot tools in controlled environments.
- **Plan for Evolving Data Privacy and Ethical Norms**: Proactively address emerging concerns related to data privacy, algorithmic bias, and transparency in district policy.

Conclusion

Navigating the AI landscape requires proactive and strategic leadership. K-12 leaders must prioritize responsible and secure AI adoption by focusing on the safety of student data, resilience of district operations, and ethical application of these technologies. Such efforts involve altering assumptions about incident response, embracing data minimization, strengthening data governance, modernizing vendor management, and championing AI literacy. Updating policies and collaborating with expert organizations are also critical actions. By embracing these principles, K-12 districts can move toward an innovative and secure AI-powered future.

Resources

- AI Risk Management Framework, Publication (U.S. Department of Commerce, National Institute of Standards and Technology)
- AI Guidance for Schools Toolkit, Publication (Teach AI)
- K-12 GenAI Readiness Checklist Questionnaire, Publication (Consortium for School Networking and Council of Greater City Schools)
- Cybersecurity Preparedness for K-12 Schools and Institutions of Higher Education, Web Page (REMS TA Center)

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

(855) 781-REMS (7367)
info@remstacenter.org
@remstacenter
https://rems.ed.gov

PLEASE NOTE: The tools and resources identified in this document are not intended as endorsements and are merely offered as examples that you may consider in your own planning efforts.