Clever

Cybersecure 2025 Action Plan

STEPS TO SECURE LEARNING FOR EVERY DIGITAL IDENTITY

Cybersecure 2025 Action Plan

STEPS TO SECURE LEARNING FOR EVERY DIGITAL IDENTITY

Recommendations for school leaders to secure digital identities in 2025

K-12 leaders are facing growing cybersecurity challenges as education gets increasingly digital—because let's be honest, you've got enough on your plate without worrying about data breaches. Dive into our **Cybersecure 2025 Report** *for an in-depth look at the current landscape of cybersecurity in education and the ever-evolving threats on student/school data.*

This guide offers actionable recommendations to help progress your district's cybersecurity practices—whether you're just starting or already on the fast track. From safeguarding student accounts to building collaborative security ecosystems, we've documented the key steps you can take this year to secure digital learning for every student (and give yourself a little peace of mind while you're at it).

Recommendations at a glance:

1. **Prioritize student account protection:** With student digital identities emerging as prime targets for cyberattacks, districts must shore up their approach to student account security.

2. **Modernize identity and access management:** Districts should adopt a zero trust security model built on modern, automated identity management.

3. **Choose classroom-friendly security solutions:** Cell phone bans can enhance focus, but districts must adopt innovative security measures to ensure student safety without relying on devices for MFA.

4. **Build a collaborative security ecosystem:** Districts need collaborative support from vendors, state agencies, and the edtech ecosystem to implement effective, transparent, and practical cybersecurity measures.

"In my work, I see many small- to medium-sized K-12 school districts starting to focus more on formalizing their cybersecurity programs, including governance from the top down. **Many district superintendents and school boards are realizing the importance of top-level support in these programs.** A good cybersecurity program is not just an IT concern but is, in fact, a strong business concern. I see districts implementing proven cybersecurity controls like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the CIS Critical Security Controls (CIS Controls) more in the coming year to help them be strategic in their efforts and investments."

- Jason Emery | Director of Cybersecurity Advisory Services Program, **Center for Internet Security**

Clever

Prioritize student account protection

Students' Digital Identities: A Prime Cyber Target

Although schools have made significant investments in stronger protections for staff, the digital identities of all students—ranging from younger grades to high school—may now be the most vulnerable aspect of the K-12 ecosystem.

Key Insights:

- A student record can be worth up to $300 on the dark web. (**source**)
- One in four districts report increased cyberattacks specifically targeting student accounts.
- Only 5% of students are protected by multi-factor authentication (MFA), compared to 90% of staff.

Steps:

1. Bring cybersecurity awareness and digital citizenship education into student curricula.
2. Implement additional layers of authentication security on student accounts (e.g. MFA).
3. Establish robust monitoring systems for student account activity.
4. Develop clear protocols for handling student-to-student security incidents.

How to approach with Clever:

Clever Classroom MFA provides age-appropriate, device-free authentication methods, including login pictures for young students and Badges for older students to provide layers of security for the Clever Portal, Google, and Entra ID accounts. Clever brings classroom-friendly cybersecurity to the forefront of your students' digital journeys without sacrificing a seamless learning experience.

Clever Access Logs provide continuous visibility into access attempts into the digital education ecosystem for enhanced security, enabling districts to maintain visibility, respond to threats, and simplify security management.

Clever

Modernize identity and access management

The Shift Toward Modern Security Architecture

Districts should progress towards a zero trust security model by building a foundation of modern identity and access management to ensure only authenticated and authorized users can access key resources. Considering known resource constraints, to do this successfully, education needs to move towards automation and simplification (e.g. cloud-based solutions and consolidated platforms) to reduce administrative overhead and gain more proactive security monitoring.
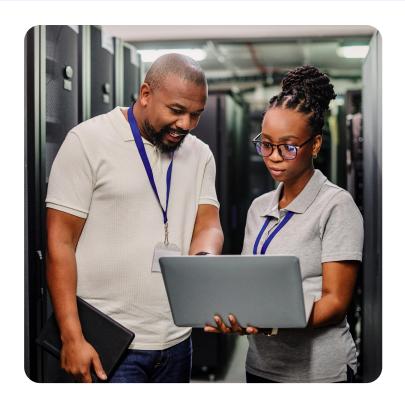
Key Insights:

- Adoption of zero trust principles is rising: 46% of districts are considering or implementing zero trust.
- 45% of districts are using or considering fully cloud-based identity solutions.
- 41% are not using risk-based or adaptive authentication yet.

Steps:

1. Consolidate and simplify tech platforms and ecosystems.
2. Automate identity and access management processes.
3. Transition to cloud-based identity management systems.
4. Implement Single Sign-On (SSO) and Multi-Factor Authentication (MFA) for all users.
5. Use role-based access controls tailored to distinct school user needs.

How to approach with Clever:

Clever is the identity platform for education. Clever can support districts and education institutions seeking to modernize identity and access management in a variety of ways from a centralized and automated account lifecycle and password management tool - Clever IDM to a multi-factor authentication solution designed for the unique needs of schools - Classroom MFA. Paired with Clever's Single-Sign On infrastructure that has powered seamless, secure connections to edtech for millions of students and teachers for over a decade, Clever delivers a comprehensive identity platform that helps you simplify and automate identity and access for education.

Clever

Choose classroom-friendly security solutions

Amidst Cell Phone Bans, Student Security Requires Innovative Solutions

The trend toward phone restrictions will require schools to rethink student-specific security solutions that work effectively — regardless of students' age — within modern classroom policies.

Key Insight:

- 60% of schools are restricting cell phone use.

Steps:

1. Avoid reliance on personal devices for MFA.
2. Introduce age-appropriate multi-factor authentication.
3. Ensure solutions are cost-effective and compatible with classroom needs.

How to approach with Clever:

Clever's Classroom MFA provides tailored authentication options for you to meet the varying needs of K-12 students, including picture matching, physical badges, 6-digit PINs, biometrics, hardware tokens, and traditional MFA methods. Classroom MFA also provides intuitive teacher and guardian support tools to unblock access for students that get stuck during logins.

Clever

Build a collaborative security ecosystem

Foster Partnerships to Strengthen District Cybersecurity

Districts shouldn't face cybersecurity challenges alone. A comprehensive strategy requires collaboration between districts, vendors, and the broader edtech ecosystem. As part of this effort, districts should understand how data is shared with applications and adopt a data minimization philosophy—sharing only the minimum data necessary to ensure security and privacy.

Key Insights:

- Staffing shortages and limited awareness among non-IT staff hinder cybersecurity progress.
- 37% of districts cite staffing shortages as their top concern.

Steps:

1. Catalog edtech tools to ensure visibility and control across your schools.
2. Use analytics to understand which tools are actively in use.
3. Work with vendors to implement transparent, practical cybersecurity measures.
4. Create systems to track and verify vendor certifications.
5. Partner with state agencies to raise awareness of emerging threats, share resources, and exchange best practices.
6. Engage with the broader edtech community to tackle staffing shortages and operational challenges.

How to approach with Clever:

Clever works with districts and partners to provide tailored security solutions and resources that address real-world challenges. By fostering collaboration, Clever ensures districts are supported in safeguarding their systems and communities. Clever's application dashboard and edtech analytics offering ensures districts have visibility into the plethora of edtech tools being utilized and accessed in their tech ecosystem.

Additional resources:

- **NIST Cybersecurity Framework Resources Alignment for K-12** (CoSN)
- **Cybersecurity Blueprint** (Clever)
- **K-12 Administrator guide to evaluating edtech vendor security** (Clever)
- **How Can Schools Assure K-12 Vendors Embrace their Cybersecurity Responsibilities?** (K12 SIX)

As of January 2025, CISA recommends that K-12 organizations take these key steps:

- Join relevant collaboration groups, such as MS-ISAC and K12 SIX.
- Work with other information-sharing organizations, such as fusion centers, state school safety centers, other state and regional agencies, and associations.
- Build a strong and enduring relationship with CISA and FBI regional cybersecurity personnel.

Clever

Clever

Clever is on a mission to connect every student to a world of learning. More than 77% of U.S. K-12 schools use Clever to power secure digital learning experiences. With Clever's layered security solutions, K-12 schools can protect district access and identities for all staff, teachers, and students. With a secure platform for schools and a network of leading application providers, Clever is committed to advancing education with technology that works for students everywhere. Clever, a Kahoot! company, has an office in San Francisco, CA, but you can visit us at clever.com anytime.

W/A Whiteboard Advisors

Whiteboard Advisors is a mission-driven communications, research, and consulting firm that supports organizations working to advance educational equity and economic mobility. Our clients include the nation's most respected philanthropies, companies, nonprofit organizations, and investors. Our work is truly multidisciplinary, sitting at the intersection of business, policy, practice, and the media.