Navigating compliance while keeping student data secure.

As federal security regulations continue to evolve, it has become more challenging for school districts to stay up to date and keep their networks secure. The right partner can help you stay compliant while protecting your students from harmful content and ensuring the privacy of all your faculty, students and staff.

Earn your E-rate certification each year.

The most important regulation for schools to keep up with is the Children's Internet Protection Act (CIPA), which requires a new certification each year.

Tips to earn your certification:

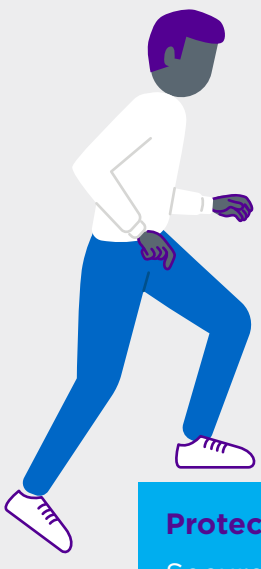
1. **Create an internet safety policy.**
   Define acceptable use and monitor children's online activities.
2. **Implement technology protection measures.**
   Block certain web content and use firewalls to prevent unauthorized access to school devices.
3. **Hold public hearings.**
   Promote transparency around your district's security compliance.

Steps to ensure compliance.

Other regulations like the K-12 Cybersecurity Act of 2021 and the Family Educational Rights and Privacy Act (FERPA) require districts to establish basic cybersecurity measures, or face fines and loss of accreditation. The best way to ensure compliance is to regularly audit and report on your district's capabilities.

Plan for threat response.

Develop and test an incident response plan, making breach reporting mandatory.



Safeguard PII.

Conduct privacy risk assessments, adopt risk-based authentication, encrypt data and implement malware protection.

Invest in impactful measures.

Deploy multi-factor authentication, implement access controls and conduct cybersecurity training.

Protect users.

Secure passwords and authentication credentials through their lifecycles by enforcing password policies like encrypting stored passwords and locking out accounts that experience suspicious login activities.

Focus on information sharing.

Join collaboration groups (e.g., MS-ISAC, K12 SIX), build relationships with regional cybersecurity personnel (e.g., CISA, FBI) and work with security organizations (e.g., fusion centers, state school safety centers, state or regional agencies).

Stay protected with our advanced solutions.

Managed SD-WAN

Virtually scale your network to meet the needs of your students and faculty and to ensure highly secure, encrypted connectivity on and off campus.

Cyber Defense

Stop cyber threats with a fully staffed Security Operations Center (SOC), powered by CyFlare, that identifies threats to your network and helps remediate them quickly.

Secure Remote User

Extend security beyond school grounds and deliver a reliable, seamless experience to remote students and faculty through verification and authentication.

DDoS Defense

Monitor your traffic in real time and automatically mitigate malicious activity to help your school district stay protected and respond to threats faster.

Ready to connect?

Give us a call at 1-888-898-4215.

Crown Castle owns, operates and leases more than 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. As an open-access broadband provider, Crown Castle's nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service, bringing information, ideas and innovations to the people and businesses that need them. Crown Castle also participates in and supports multiple Federal Broadband programs.