

Keeping Students Safe Online and Meeting CIPA Compliance With Fortinet

Executive Summary

Schools are expected to keep their students physically and digitally safe, even with increasing numbers of devices connecting to their networks. In addition, 1:1 initiatives have accelerated rapidly since 2020, and students are accessing lessons and completing homework online. These challenges make complying with the Children’s Internet Protection Act (CIPA) more complicated, and pervasive internet use by tech-savvy students makes it more important than ever. Essentially, CIPA requires K–12 schools and libraries to certify that they are enforcing internet safety policies in order to be eligible for E-rate discounts.

Much has changed since CIPA was enacted by the U.S. Congress in 2000, but the rules enforced by the Federal Communications Commission remain in place. CIPA has become synonymous with “web filtering,” which relies heavily on text and object patterns in images to provide restrictions where needed. This service works well when traffic is open and easily analyzed by filtering software or hardware. This is not the case when traffic or content websites themselves are encrypted with SSL/TLS encryption. In the early 2000s, very few websites or even software browser companies supported SSL encryption; fast-forward to today, and 95% of all internet-based traffic is encrypted when processed through search engines, per Google HTTPS statistics.¹

Fortinet Solutions

Fortinet offers products that can help you achieve CIPA compliance for your school or library.

FortiGate: Our E-rate-eligible, next-generation firewalls deliver top-rated network security, as well as the ability to monitor your network and filter even encrypted internet traffic for inappropriate content in real time.

FortiClient: Our endpoint protection platform delivers easy to manage, automated, customizable antivirus, web filtering, application control, IPS, and more, for endpoints on- or off-network, including Chromebooks.

Linksys HomeWRK for Education | Secured by Fortinet: This is the only all-in-one solution that includes intelligent content filtering and malware protection. It is designed to help students who otherwise don’t have adequate internet access get reliable connectivity and security at home.

FortiMail: Email is the most frequently used delivery method for malware. Our secure email gateways feature high-performance, top-rated security effectiveness and data loss prevention (DLP).

FortiWeb: Our web application firewalls (WAFs) monitor, allow, or block application traffic by categories. It can prevent the use of unwanted applications, including proxy apps and HTTPS messaging apps.

CIPA Requirements

Schools and libraries subject to CIPA are required to adopt a policy that addresses all of the following:

- Access by minors to inappropriate matter on the internet and World Wide Web.
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- Unauthorized access, including “hacking” and other unlawful activities by minors online.
- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Access to materials harmful to minors. (Security measures must be able to block or filter pictures that are obscene or contain child pornography.)
- Failure to submit certification: Any library or school that fails to submit the certification requirements shall be ineligible for funding under the E-Rate program.
- Failure to comply with certification: Any school or library that “knowingly fails to ensure the use of its computers”² in compliance with these requirements not only loses eligibility for funding, but must reimburse the E-Rate fund for discounts received during the period covered by such certification. Additionally, other laws, including criminal laws, provide serious penalties for providing false statements to the federal government.

FortiSandbox: Proactive advanced threat protection (ATP) stops the latest and most sophisticated threats.

FortiEDR: Comprehensive endpoint security that can prevent ransomware from exfiltrating children’s private and personal data.

How Fortinet Products Address Specific CIPA Requirements

CIPA Requirements	Addressed With	
Prevent minors from accessing inappropriate matter on the internet and World Wide Web	<p>FortiGate:</p> <ul style="list-style-type: none"> Web filtering to block sites under inappropriate categories such as adult/mature content. Manual website blacklisting to block webpages by keywords or URLs. Safe search enforcement to rewrite search queries with Safe Search option to deliver child-appropriate results. 	<p>FortiWeb:</p> <ul style="list-style-type: none"> Prevents the use of unwanted applications, including proxy apps and HTTPS messaging apps. Linksys HomeWRK for Education Secured by Fortinet. Web filtering to block sites under inappropriate categories such as adult/mature content. <p>Linksys HomeWRK:</p> <ul style="list-style-type: none"> Web filtering to block sites under inappropriate categories such as adult/mature content.
Address the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications	<p>FortiGate:</p> <ul style="list-style-type: none"> Antivirus to detect malicious attachments or file transfers over electronic communications. Anti-spam, DLP to stop malicious or inappropriate content. Web filtering to restrict social media and online communication sites. 	<p>FortiSandbox:</p> <ul style="list-style-type: none"> Sandboxing to stop advanced threats that evade traditional security measures. <p>FortiMail:</p> <ul style="list-style-type: none"> Secure email gateway to protect from email-borne threats.
Prevent unauthorized access, including “hacking” and other unlawful activities by minors online	<p>FortiGate:</p> <ul style="list-style-type: none"> Firewall to enforce access to other networks and internet. User authentication can also be implemented. Application control to prevent the use of malicious or inappropriate applications. IPS to detect and block unlawful activities. 	<p>FortiEDR:</p> <ul style="list-style-type: none"> Detects ‘hacking’ activities by minors online. <p>Linksys HomeWRK:</p> <ul style="list-style-type: none"> SSL decryption helps catch malware and malicious content from HTTPS sites that bypass filtering.
Prevent unauthorized disclosure, use, and dissemination of personally identifiable information (PII) regarding minors	<p>FortiGate:</p> <ul style="list-style-type: none"> Firewall to prevent unauthorized access to internal hosts. Antivirus to mitigate malicious code infections that allow external control. DLP to protect against servers and terminals from disclosing personal information. 	<p>FortiMail:</p> <ul style="list-style-type: none"> Integrated, robust data protection to prevent disclosure of confidential information.
Address measures designed to restrict minors’ access to materials that are harmful to minors	<p>FortiGate:</p> <ul style="list-style-type: none"> Web filtering to block sites under inappropriate categories such as violent content. Manual website blacklisting to block web pages by keywords or URLs. Safe search enforcement to rewrite search queries with Safe Search option to deliver child-appropriate results. <p>FortiClient:</p> <ul style="list-style-type: none"> Device-level security and web filtering, IP reputation, and application control to keep students from accessing inappropriate sites, even when off the network. 	<p>FortiWeb:</p> <ul style="list-style-type: none"> Prevents the use of unwanted applications, including proxy apps and HTTPS messaging apps. <p>Linksys HomeWRK:</p> <ul style="list-style-type: none"> Application control can pre-define and block categories of harmful applications and protect students and teachers from malicious content.

Visit Fortinet at <https://www.fortinet.com/solutions/industries/education/k12> for more information.

¹ Jeff Costlow, “How Decryption of Network Traffic Can Improve Security,” InfoSec Insider, Nov. 30, 2021.

² “Children’s Internet Protection: An Analysis,” Legal Counsel for the American Library Association.

