The Children's Internet Protection Act for K-12 Schools

Understanding and developing strategies that benefit your community

Creating safe K-12 schools for children

K-12 Schools are centers of Internet connectivity for support of pedagogy, online research, and other educational activities. This has created a fundamental challenge: providing information to all while "protecting against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to use of computers with internet access by minors – harmful to minors. "Minor" is defined as any individual who is under the age of 17."[1]

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000. In 2001, the FCC issued rules for the implementation of CIPA, and in 2011, the FCC provided additional CIPA guidance. Schools must have an Internet safety policy that provides protection required to: 1) block or filter Internet access to pictures defined as obscene, child pornography, or harmful to minors. Before adopting this Internet safety policy, schools must give ample notice to facilitate a minimum of one public hearing or meeting to communicate the proposed safety measures.

Nearly two decades later, CIPA still poses a challenge for schools as compliance with the law must be balanced against every changing online threats. The evolution of technology has made this easier. And there's a potential opportunity within CIPA: compliance can open doors for federal funding opportunities that can help schools provide increased online learning opportunities.

CIPA Highlights

- CIPA imposes requirements on schools and libraries that receive discounts for Internet access or internal connections through the federal E-rate program.
- CIPA requires K-12 schools to certify they have an Internet safety policy that includes technology protection measures. These measures must block or filter Internet access to images that are obscene, child pornography or harmful to minors.
- An "authorized person" can disable block- ing or filtering to allow unfettered use by adults for "bona fide research or other lawful purposes," according to the FCC.
- The law requires K-12 schools to monitor Internet use by minors. But, there is no requirement to track Internet use by minors or adults.

Strategies for CIPA

Any school or library receiving either Internal connections or Internet access must:

- Filter all Internet access.
- Draft an Internet Safety Policy (adopted after public hearing) that addresses required elements.
- Schools' (not libraries) Internet Safety Policy must address:
    - teaching minors about appropriate online behavior.
    - interacting with others online and cyberbullying awareness and response.
- Schools must teach online safety as a prerequisite to receipt of E-rate funding.

CIPA's provisions requiring Internet filtering don't specify the technology to be used, according to the ALA: "Although the law clearly requires the use of filtering or blocking technology, it does not require the use of specific filtering software or services. Instead, CIPA requires schools or libraries covered by the new requirements to certify they are using technology that blocks or filters access to visual depictions of the type specified in the legislation."[2]

CIPA uses the federal criminal definitions for obscenity and child pornography, and there are exceptions for libraries. Please see the CIPA library guide.

Decisions about what matter is inappropriate for minors are made by the local community.

E-rate program rules specify that "determination regarding matter inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination."[3]

The Administrative Authority for a school or library is the entity that must make the relevant certification for the purposes of CIPA. This authority may be different for a variety of reasons. However, this authority is also the responsible agent providing for the public meeting or hearing that addresses Internet safety and the proposed technology solution for CIPA compliance.

Thankfully, modern filtering software is frequently updated by providers and has grown more sophisticated in the years since CIPA's passage. So, what once took lots of IT resources can now be easily addressed.

Resources

- FCC CIPA Guidelines
- E-rate
- American Library Association (ALA)
- USAC CIPA Guidance

Endnotes:

1. https://www.usac.org/e-rate/applicant-process/starting-services/cipa/

2. https://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/cipa/cipatext.pdf

3. https://www.usac.org/e-rate/applicant-process/starting-services/cipa/

This piece contains abbreviated content developed and written by the Center for Digital Education Content Studio for use in the brief CIPA and Libraries: Challenges and Opportunities, with information and input from Cisco. The information provided in this paper does not, and is not intended to, constitute legal advice; instead, all information is for general informational purposes only.

CIPA and E-rate

In 2014, the FCC modernized the E-rate program, increasing the annual spending cap and emphasizing broadband capacity and Wi-Fi. According to numerous reports, the changes were beneficial to K-12 schools and libraries. For the first time in over 15 years, mostly all E-rate applicants can receive E-rate funding.

The result was that all schools and libraries, whether in remote rural areas or urban centers, had access to much-needed funding for their in- building network requirements.

Updated changes for eligible E-rate applicants include a minimum funding floor of $25,000 when their E-rate Category 2 budget does not reach this benchmark figure. Regardless of size, all schools and libraries can use their funding in the buildings or locations that need it the most.

CIPA requires libraries and schools which receive E-rate funding to be compliant with its regulations as a condition of receiving funding.

Get started

To begin your E-rate journey, visit:

Cisco.com/go/erate