CIPA

(Children's Internet Protection Act)

E-Rate Instruction Manual

CIPA (Children's Internet Protection Act)

Overview:

Applicants must enforce a policy of Internet safety and certify compliance with the Children's Internet Protection Act (CIPA) to be eligible for discounts. CIPA was signed into law on December 21, 2000. To receive support for Category One Internet access and all Category Two services – internal connections, managed internal broadband services, and basic maintenance of internal connections, school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. The relevant authority with responsibility for administration of the eligible school or library (hereinafter known as the Administrative Authority) must certify the status of its compliance for the purpose of CIPA in order to receive Universal Service support.

In general, school and library authorities must certify either that they have complied with the requirements of CIPA, that they are undertaking actions, including any necessary procurement procedures, to comply with the requirements of CIPA, or that CIPA does not apply to them because they are receiving discounts for telecommunications services only.

Requirements

CIPA requirements include the following three items:

1. Internet Safety Policy

Schools and libraries receiving Universal Service discounts are required to adopt and enforce an Internet safety policy that includes a technology protection measure that protects 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.

CIPA (Children's Internet Protection Act)

Internet Safety Policy, continued

The Internet safety policy must address all of the following issues:

- 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
- Measures designed to restrict minors' access to materials harmful to minors

For schools, the policy must also include monitoring the online activities of minors.

Note: As of July 1, 2012, as part of their CIPA certification, schools are also required to certify that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

2. Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters Internet access.

The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. For example, a library that uses Internet filtering software can set up a process for disabling that software upon request of an adult user, through use of a sign-in page where an adult user can affirm that he or she intends to use the computer for bona fide research or other lawful purposes.

CIPA (Children's Internet Protection Act)

Technology Protection Measure, continued

CIPA uses the federal criminal definitions for obscenity and child pornography. The term "harmful to minors" is defined in the statute and in the E-rate rules as "any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors."

Decisions about what matter is inappropriate for minors must be made by the local community. E-rate program rules specify that the library or other authority for making the determination shall make ['a] determination regarding matter inappropriate for minors."

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. For private schools, public notice means notice to their appropriate constituent group. Additional meetings are not necessary – even if the policy is amended – unless required by local or state rules or the policy itself.

Certification for Undertaking Actions

Below is the appropriate certification that the Administrative Authority must make for "undertaking actions" from the Federal Communications Commission, FCC 01-120 Order, released on April 5, 2001:

"I certify that, as of the date of the start of discounted services, pursuant to the Children's Internet Protection Act, as codified at 47 U.S.C. Section 254(h) and (l), the recipient(s) of service represented in the Funding Request Number(s) on this FCC Form 486 is (are) undertaking such actions, including any necessary procurement procedures, to comply with the requirements of CIPA for the next funding year, but has (have) not completed all requirements of CIPA for this funding year."