USAC CONNECTION

SCHOOLS AND LIBRARIES PROGRAM

NEWS BRIEF

SPECIAL EDITION

July 21, 2016

Children's Internet Protection Act (CIPA) Guidance for Libraries

Libraries receiving E-rate discounts on products and services that provide access to the Internet must comply with the requirements of the Children's Internet Protection Act (CIPA). These products and services include Category One Internet access and all Category Two (C2) services – internal connections, managed internal broadband services, and basic maintenance of internal connections. We are providing the guidance below to enable libraries interested in applying for Internet access and/or C2 services to understand what they need to do to be compliant with CIPA.

What is required for a library to be compliant with CIPA?

CIPA has three basic requirements:

1. Internet Safety Policy: Libraries must adopt and enforce an Internet safety policy that includes five specific elements and a technology protection measure or filter (see below). Libraries that already have an Internet safety policy or acceptable use policy can amend their existing policy to include the required elements. The policy must address the following:

- Access by minors to inappropriate matter on the Internet or World Wide Web;
- 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, dissemination of personal information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.

Note: "Minor" is defined as any individual who has not attained the age of 17 years.

2. Technology Protection Measure: Libraries must enforce the use of a technology protection measure (i.e., a filter or a technology that blocks or filters Internet access) on all of their computers with Internet access. The filter must protect against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to the use of computers with Internet access by minors – "harmful to minors." The filter can be disabled during use by an adult to enable access for bona fide research or other lawful purpose.

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."

E-rate program rules allow libraries to determine their own processes for disabling technology protection measures 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.

3. Public Notice and Meeting or Hearing: Libraries must provide reasonable public notice and hold at least one public meeting or hearing to address the proposed filter and the Internet safety policy. Additional meetings are not necessary – even if the policy is amended – unless required by local or state rules or the policy itself.

Who certifies compliance with CIPA?

The library's administrative authority – the library, library board, or other authority responsible for the administration of the library – must certify one of the following:

1. The library has complied with the CIPA requirements;
2. The library is undertaking actions to comply with the CIPA requirements; or
3. CIPA does not apply because the library is receiving E-rate discounts only for telecommunications services.

The administrative authority can certify on the FCC Form 486 if it is applying for E-rate discounts directly (i.e., if it is the billed entity). If the administrative authority is not applying directly – for example, if a consortium or a town or county government applies on behalf of the library – the administrative authority certifies on the FCC Form 479 and provides a copy of this form to the entity applying on its behalf.

When does the library need to be compliant with CIPA?

In the first year a library receives E-rate funding for Internet access and/or C2 services, the library can certify that it is undertaking actions to be compliant with CIPA for the next funding year. In the second (next) funding year, the library must certify that it is compliant with CIPA.

Can CIPA issues be corrected?

It depends on the issues that need correction. The FCC has directed USAC to give applicants the opportunity to correct minor errors that could result in violations of the CIPA rules before instituting recovery of E-rate funds. Correctable errors are those that are immaterial to CIPA compliance. For example, if a school has complied in practice with its CIPA certification, but inadvertently left out one of the details of its practice in its written Internet safety policy, the FCC would consider that to be an immaterial error that could be corrected. Also, since 2011, entities have been required, at a minimum, to keep at least some record of when the public notice and meeting or hearing took place (e.g., a copy of the meeting agenda, or a newspaper article announcing the meeting or hearing). However, if a school or library cannot locate a record of a public notice and meeting or hearing that was held after August 2004, the school or library can correct its failure to document its public meeting or hearing by providing a public notice and holding a meeting or hearing. These are just two CIPA issues that have been addressed by the FCC, but there may be others that can be corrected.

What documentation does the library need to maintain to demonstrate CIPA compliance?

Below is a list of the documentation that will be requested to demonstrate CIPA compliance during an audit. The library should retain copies of the documentation for each funding year where a CIPA certification is required. Note that documents must be retained for at least 10 years after the latter of the last day of the applicable funding year or the service delivery deadline for the funding request.

- A copy of the Internet safety policy.
- Documentation that the library gave public notice and held a public meeting or hearing on the policy. For example, the library could demonstrate the public notice with a copy of a website announcement for a regular library board meeting open to the public where the policy will be discussed, or an advertisement in a local newspaper of a county government meeting or hearing where the policy appears as an agenda item. The library could also demonstrate that the meeting or hearing occurred with a copy of the minutes of the meeting or hearing and the date it occurred.
- Documentation of the adoption of the policy – for example, approval in the minutes of the meeting or hearing, or documented adoption by the library board.
- A description of the filter.
- A report or other documentation on the use of the filter. The documentation should show that the filter was installed and working during the funding year. For example, a library that purchased filtered Internet access could archive a sampling of reports from the service provider of Internet sites blocked, or bills from the service provider verifying that the filter was operational. If a library purchased its own filter, it could archive logs produced by its IT staff showing the hours the filter was engaged.

- Copies of the FCC Form 479 and/or FCC Forms 486, as applicable.

If you have questions about this information or for additional help, please contact USAC's Client Service Bureau at (888) 203-8100. You can also refer to the CIPA guidance document on the USAC website.