

CIPA (Children's Internet Protection Act)

In order for schools and libraries to receive E-rate funding for Internet Access, Internal Connections or Basic Maintenance of Internal Connections, they must be compliant with the Children's Internet Protection Act (CIPA) which requires an Internet Safety Policy and the use of a filtering mechanism on all computers.

Important Update to Existing CIPA Law:

The FCC has released its long-awaited Order to implement the CIPA (Children's Internet Protection Act) Amendments passed by Congress in 2008. The new law, entitled "Protecting Children in the 21st Century Act," contained a provision requiring schools' Internet Safety Policies to include "... educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response." Essentially this means that schools are required to teach online safety to students as a prerequisite to receiving E-rate funding for Internet access or Priority 2 funding. Below is an FAQ that contains details on the new FCC rules. The full Order is available at: http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0811/FCC-11-125A1.pdf.

1) When do the requirements become effective?

-- The new requirement becomes effective for E-rate Funding Year 2012 which begins July 1, 2012. This means you should have your Internet Safety Policy updated before this date and be prepared to implement your online behavior/cyberbullying curriculum for the beginning of the 2012 school year.

2) Are schools required to hold a new public hearing to amend their Internet Safety Policy?

-- No. Applicants that have existing and properly adopted Internet Safety Policies will not be required to hold new public hearings to amend their policies to comply with the new rules. Applicants that are new to the E-rate program and have never held a public hearing or adopted their Internet Safety Policy remain bound by the public notice and public hearing requirements.

3) What must be included in the Internet Safety Policy?

-- Schools' Internet Safety Policies must include monitoring the online activities of minors and must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Although the ISP must provide for the development and use of educational materials related to appropriate online behavior/cyberbullying, the policy itself does not have to include the actual materials. If the curriculum and materials are not included, they must be documented elsewhere.

4) What must be included in the online behavior/cyberbullying curriculum and with what frequency must the material be taught?

-- The FCC decided it is entirely up to the local school board to decide how to implement the new online behavior/cyberbullying curriculum. Further, the Commission did not offer any formal definition of cyberbullying or social networking. In an effort to clear-up a common misconception, the FCC specifically noted that Facebook or MySpace are not required to be blocked under FCC rules.

5) How long must schools keep a copy of their Internet Safety Policy?

-- Schools must retain their Internet Safety Policy documentation for at least five years after the last date of service for a particular funding year. For example, if a school held a public hearing and adopted its Internet Safety Policy in 2001 and relied on that same policy to make its Form 486 CIPA certification in FY 2011, the school must retain its Internet safety policy documentation (from 2001) for five years after the last day of service for FY 2011, which would be until June 30, 2016. If you don't have this documentation, you should issue a new public notice, hold a new public hearing, and adopt your current Internet Safety Policy to become compliant.

6) Are schools required to send USAC or the FCC a copy of their Internet Safety Policy?

-- No. But schools must provide the FCC or USAC with a copy of their Policy upon request.

7) Did the FCC clarify the filtering rules pertaining to portable devices?

-- The FCC stated they intend to request public comment in a future proceeding to consider whether CIPA/filtering applies to portable devices owned by students/staff/library patron-owned (such as laptops and cellular phones) when those devices are used in a school or library to obtain E-rate-funded Internet access.

8) Do the new online behavior/cyberbullying requirements pertain to libraries?

-- No. The new rules are only applicable to schools.

9) What free online materials including age-appropriate lesson plans are available?

- <http://www.staysafeonline.org/content/k-12-educators>
National Cyber Security Alliance: Public/Private Partnership including Dep't. Homeland Security, corporate sponsors such as Symantec, CISCO, Microsoft, SAIC, EMC, McAfee) and other nonprofits.
- <http://www.media-awareness.ca/english/resources/educational/lessons/cyberbullying.cfm>
Media Awareness Network : MNet is a Canadian non-profit organization that has been pioneering the development of media and digital literacy programs since its incorporation in 1996.
- <http://www.cybersmartcurriculum.org/>
Free curriculum CyberSmart! Cyberbullying Package; endorsed by National School Boards Association, Technology Leadership Network and others

Overview of CIPA

CIPA was signed into law on December 21, 2000. To receive support for Internet access and internal connections services from the Universal Service Fund (USF), 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 must certify the status of its compliance for the purpose of CIPA in order to receive USF 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 of CIPA

CIPA requirements include the following three items:

1) Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters Internet access. It must protect 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. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

2) Internet Safety Policy

The Internet safety policy must address 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
- Education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

3) Public Notice and Hearing

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed technology protection measure and Internet safety policy. The hearing requirement may be satisfied if your school board meeting has the opportunity for public input and notice of the Board vote on the Internet Safety Policy is provided to the public in advance of the school board meeting. Adoption of amendments to the Internet Safety Policy should also comply with the public notice/hearing requirement.

Definitions of First, Second, and Third Funding Years

CIPA provides that, in the first funding year following the effective date of CIPA (April 20, 2001) in which you are "applying" for funds, you need not be fully compliant with CIPA's requirements but can certify that you are undertaking actions to be in compliance for the next funding year. You may also make this certification in your second funding year for purposes of CIPA if you seek a waiver due to state or local procurement rules or regulations or competitive bidding requirements. Applicants, therefore, need to determine their "first," "second," and "third" funding years after the effective date of CIPA (April 20, 2001) in which their school or library is "applying" for support AND must also understand what "applying" for support means in this context.

Applying for support. For the purpose of CIPA requirements, a school or library that is a recipient of service is considered to have "applied" for support in a funding year only when a *Receipt of Service Confirmation Form* (Form 486) for a funding request for Internet access or internal connections has been successfully processed into the USAC system.

Determination of your first funding year for purposes of CIPA. The first funding year after the effective date of CIPA (April 20, 2001) in which your school or library is "applying" for support (i.e., in which a Form 486 is successfully processed) for Internet access or internal connections is the **first funding year** for the purpose of CIPA. Once your first funding year is established, the next two funding years will be your second and third funding years for the purpose of CIPA. In the first funding year, the applicant must be in compliance with CIPA or undertaking actions to comply with CIPA in order to receive support for Internet access or internal connections services.

Once the first funding year is established, the funding year immediately following the first funding year becomes the **second funding year** for purposes of CIPA.

If the school or library "applies" for support for Internet access or internal connections in the second funding year, its Administrative Authority must certify compliance with CIPA unless state or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification. If in the second funding year, the Administrative Authority for the school or library is unable to make the certification otherwise required due to state or local procurement rules or regulations or competitive bidding requirements, the Administrative Authority must submit a CIPA waiver on Form 486 Item 6C or the *Certification by Administrative Authority to Billed Entity of Compliance with the Children's Internet Protection Act* (Form 479) Item 6d, as appropriate. The Administrative Authority must also certify that the affected schools or libraries will be brought into compliance with the CIPA requirements before the start of the third funding year after the effective date of CIPA (April 20, 2001) in which they apply for discounts. **When the waiver box in Item 6C on Form 486 or Item 6d on Form 479 is checked for the second funding year after the effective date, the Administrative Authority should certify for the second funding year that the schools or libraries under its administrative authority are "undertaking actions" to comply with CIPA for the next funding year.**

The **third funding year** for purposes of CIPA is the funding year immediately following the second funding year. If the school or library "applies" for support for Internet access or internal connections in the third funding year, it must be in compliance with CIPA.

The school or library must be in compliance with CIPA for any funding year thereafter.

Appropriate Certification for "Undertaking Actions"

Here is the appropriate certification that Administrative Authorities must take for "undertaking actions" from the FCC Order released 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. § 254(h) and (l), the recipient(s) of service represented in the Funding Request Number(s) on this 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.

Documentation for "Undertaking Actions"

For a school or library to be able to make the certification quoted above, it must be able to demonstrate that action was taken by the start of services. USAC will not request this documentation as part of the Form 486 filing process but the school or library must maintain this documentation in its files for audit purposes.

An undertaken action is an action that can be documented and that moves the school or library toward compliance. Note that if a school or library has already provided reasonable public notice and at least one public hearing or meeting relating to an Internet safety policy and technology protection measure that meets all the requirements listed above, that school or library has complied with the public notice and hearing requirements of CIPA. If a school or library has not met those conditions, the statute requires that the school or library provide the required notice and hearing or meeting.

Following are a few examples of documentation that could demonstrate that a school or library is "undertaking actions" to comply with CIPA:

- A published or circulated school or library board agenda with CIPA compliance cited as a topic
- A circulated staff meeting agenda with CIPA compliance cited as a topic
- A service provider quote requested and received by a recipient of service or Billed Entity which contains information on a technology protection measure

- A draft Request for Proposals or other procurement procedure to solicit bids for the purchase or provision of a technology protection measure
- An agenda or minutes from a meeting open to the public at which an Internet safety policy was discussed
- An agenda or minutes from a public or non-public meeting of a school or library board at which procurement issues relating to the acquisition of a technology protection measure were discussed
- A memo to an administrative authority of a school or library from a staff member outlining the CIPA issues not addressed by an Acceptable Use Policy currently in place
- A memo or report to an administrative authority of a school or library from a staff member describing research on available technology protection measures
- A memo or report to an administrative authority of a school or library from a staff member that discusses and analyzes Internet safety policies in effect at other schools and libraries

This list is not meant to be exhaustive.

Remember that such actions must occur before the start of services in order for discounts to be paid back to the Service Start Date reported on the Form 486.

Although such steps constitute examples of actions undertaken in order to be able to make the necessary certification in the first funding year, schools and libraries should be prepared to take all subsequent measures so that by the start of services in second funding year they will be in full compliance (unless they obtain a waiver).