

Pre-Commitment CIPA Review

The Children's Internet Protection Act (CIPA) requires schools and libraries receiving discounts on Internet Access, Internal Connections, and/or Basic Maintenance of Internal Connections services to 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.

Determination of your first, second, and third funding years for purposes of CIPA

The first funding year after the effective date of CIPA (April 20, 2001) in which you apply for support for Internet access, Internal Connections, or Basic Maintenance of 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, you 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.

If you apply for support for Internet access, Internal Connections, or Basic Maintenance of Internal Connections in the second funding year, you 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 you are unable to make the certification, you must **submit a CIPA waiver** on Form 486 Item 6b or 6c or Form 479 Item 6d or 6e, as appropriate. You must also certify that you will become compliant with CIPA requirements before the start of the third funding year.

The third funding year for purposes of CIPA is the funding year immediately following the second funding year. If you apply for support for Internet access, Internal Connections, or Basic Maintenance of Internal Connections in the third funding year, you must be **in compliance** with CIPA.

Listed below are the three requirements all applicants must meet in order to be considered CIPA compliant. Were you granted a CIPA waiver on Form 486 Item 6b or 6c or Form 479 Item 6d or 6e as described above? Yes _____ No _____

Technology Protection Measure (Filter)

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.

- Do you have a technology protection measure in place? Yes _____ No _____
- Please provide documentation that demonstrates you have a specific technology protection measure in place that blocks or filters Internet access (e.g., invoice for Internet filtering services, work orders showing when the filter was installed or will be installed, and/or a report demonstrating the web sites that have been filtered, etc.).

Public Notice and Public Hearing

CIPA requires that a 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.

- Have you provided reasonable public notice and held at least one public hearing to address a proposed technology protection measure and Internet safety policy prior to the start of your second funding year of CIPA or prior to the start of your third funding year of CIPA if granted a waiver, as described above?
- Provided Reasonable Public Notice: Yes _____ No _____
- Held at least one Public Hearing: Yes _____ No _____
- Provide supporting documentation (e.g. newspaper references, School Board letter or agenda, School Board meeting minutes).

Internet Safety Policy

An Internet Safety policy must address the following five issues:

1. Access by minors to inappropriate matter on the Internet and World Wide Web
 1. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
 2. Unauthorized access including "hacking" and other unlawful activities by minors online
 3. Unauthorized disclosure, use, and dissemination of personal information regarding minors
 4. Measures designed to restrict minors' access to materials harmful to minors
- Did you have an Internet Safety Policy in place prior to the start of your second funding year of CIPA or prior to the start of your third funding year of CIPA if granted a waiver, as described above? Yes _____ No _____
 - Provide a copy of the **most current** version of your Internet Safety policy.
 - If your policy was revised **after the start of services** for this Funding Year, please provide a copy of your **previous** Internet Safety Policy upon which the revised policy was based.