

Overview of CIPA

The Children's Internet Protection Act (CIPA) was signed into law on December 21, 2000. Under CIPA, no school or library may receive discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology (see below). This Internet Safety Policy must protect against access, through computers with Internet access, to visual depictions that are obscene, child pornography, or (in the case of use by minors) harmful to minors. The school or library must also certify that it is enforcing the operation of such filtering or blocking technology during any use of such computers by minors. The law is effective for Funding Year 2001 (07/01/2001 to 06/30/2002) and for all future years. Schools and libraries receiving only Telecommunications Services are excluded from the requirements of CIPA.

For the first Funding Year (Funding Year 2001 for Year 2001 applicants), applicants must certify on their Form 486 either that they are in compliance with CIPA, or that they are undertaking actions to put into place an Internet Safety Policy and to procure the filtering or blocking technology. For the second year (for most applicants, Funding Year 2002), they must certify on their Form 486 that they are in compliance with CIPA in order to receive universal service discounts.

However, if state or local procurement rules or regulations or competitive bidding requirements prevent the making of the required CIPA certifications, applicants may seek a waiver and provide notification that they *will be in compliance before the start of the third Funding Year (for most applicants, Funding Year 2003.)* In general, local communities are responsible for determining what constitutes prohibited material and appropriate actions by schools and libraries.

Guidance on CIPA Certifications

A library/school receiving E-rate discounts for these services is still required to have an Internet safety policy that addresses:

- (1) access by minors to inappropriate matter on the Internet and World Wide Web,
- (2) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications,
- (3) unauthorized access, including hacking, and other unlawful activities by minors online,
- (4) unauthorized disclosure, use, and dissemination of personal identification information regarding minors, and
- (5) measures designed to restrict minors' access to materials harmful to minors.

Section 254(l) also includes a public notice and hearing/meeting requirement, which remains in force.

Sample Internet Acceptable Use Policy

Note: The examples below meet the minimum Federal requirements. Your own Internet safety policy may be broader, but you should review it to insure it includes these minimum elements.

Example: All “Student Expectations in Use of the Internet” listed below are not applied to the “Staff Expectations in Use of the Internet” because the law does not require it. In your own policy, you might wish to apply these expectations to Staff as well as Students in use of the Internet.

Sample policy for a School Receiving E-rate Funding

An Internet Acceptable Use Policy (AUP) is required for schools and libraries receiving the E-rate. The E-rate requirements list several specific items that must be addressed in the policy. To help schools and libraries understand what requirements apply to them, FilteringInfo.org has created a sample policy that covers these minimum policy requirements:

- Enforce use of a technology protection measure that blocks or filters Internet access when in use by minors. A minor is defined in the legislation as "any individual who has not attained the age of 17 years."
- Address access by minors to inappropriate material.
- Address access by minors to material harmful to minors.
- Address safety of minors when using e-mail, chat, etc.
- Address unauthorized/unlawful use by minors.
- Address disclosure of personal info by minors.
- Provide means for monitoring access by minors. However, the legislation states that "Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user."

Sample Policy

Below is a sample policy that you may use to craft your own Internet Acceptable Use Policy (AUP). Please feel free to copy any and all of the language below to help you create and edit your own policy document to fit your particular needs. Note that the placeholder [YOUR SCHOOL] is meant to be replaced with the name of your organization. Also, carefully review the information in your policy to be sure that your district or local governing body is in accordance with the language.

[YOUR SCHOOL] Policy on Internet Access

Internet users are expected to use the Internet as an educational resource. The following procedures and guidelines are used to help ensure appropriate use of the Internet at [YOUR SCHOOL].

Student Expectations in Use of the Internet

- a. Students shall not access material that is obscene, pornographic, child pornography, "harmful to minors", or otherwise inappropriate for educational uses.
- b. Students shall not use school resources to engage in "hacking" or attempts to otherwise compromise system security.
- c. Students shall not engage in any illegal activities on the Internet.
- d. Students shall only use electronic mail, chat rooms, and other forms of direct electronic communications for school-related purposes.
- e. Students shall not disclose personal information, such as name, school, address, and telephone number outside of the school network.

Any violation of school policy and rules may result in loss of school-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

Staff Expectations in Use of the Internet

- a. Staff shall not use access material that is obscene or is child pornography.

Any violation of school policy may result in loss of school-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices. When and where applicable, law enforcement agencies may be involved.

Enforcement of policy

- a. [YOUR SCHOOL] uses a technology protection measure that blocks or filters Internet access to block access to some Internet sites that are not in accordance with the policy of [YOUR SCHOOL].
- b. The technology protection measure that blocks or filters Internet access may be disabled by a [YOUR SCHOOL] staff member for bona fide research purposes by an adult.
- c. A [YOUR SCHOOL] staff member may override the technology protection measure that blocks or filters Internet access for a student to access a site with legitimate educational value that is wrongly blocked by the technology protection measure that blocks or filters Internet access.
- d. [YOUR SCHOOL] staff will monitor students' use of the Internet, through either direct supervision, or by monitoring Internet use history, to ensure enforcement of the policy.

[YOUR SCHOOL] Internet Acceptable Use Policy, Approved by [YOUR SCHOOL BOARD], [On this date]