

CIPA (Children's Internet Protection Act)

In order for schools and libraries to receive E-rate funding for Internet Access, Internal Connections, Basic Maintenance of Internal Connections or Managed Internal Broadband Services, they must be compliant with the Children's Internet Protection Act (CIPA).

Overview of CIPA

CIPA was signed into law on December 21, 2000, and updated in October 2008. To receive support for Internet Access, Internal Connections, Basic Maintenance of Internal Connections or Managed Internal Broadband 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, and are educating minors about online safety and cyber bullying. 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 on the Form 486 in order to receive USF support.

In general, school and library authorities must certify either that they have complied with the requirements of CIPA. In rare cases, brand new applicants may certify that they are undertaking actions, including any necessary procurement procedures, to comply with the requirements of CIPA. Alternatively, if the school or library is receiving E-rate discounts on telecommunications services only, then they may certify that CIPA does not apply to them.

Requirements of CIPA

CIPA requirements include the following three items:

1) *A Technology Protection Measure (Filtering)*

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 (only) engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

Q & A

Based on unofficial FCC guidance, below is a Q & A that seeks to clarify the most common CIPA filtering questions:

1. Are school (or library) owned computers/devices used on-campus required to be filtered?

-- Yes.

2. Are school-owned computers/devices used off campus required to be filtered when using a privately-purchased (non-school) Internet connection?

-- The current rules do not specifically address this issue. The CIPA statute says all school owned computers must be filtered and does not distinguish between on campus and off campus use. A best practice is for all school-owned computers be filtered wherever they're used, but the issue is officially considered 'open.'

3. Are privately-owned computers/devices using the school's Internet access required to be filtered?

-- This is considered an 'open' issue as of October 2014. The FCC stated in August 2011 that they intended to request public comment in a future proceeding to consider whether CIPA/filtering applies to portable devices/computers owned by students/staff/library patrons when those devices are using Internet access that is funded by E-rate. No request for comment has been released by the FCC as of October 2014 therefore this is not an E-rate requirement.

4. Are privately-owned computers/devices using a privately-purchased Internet connection (not the school's) required to be filtered when being used on campus?

-- The FCC has not addressed this issue. (While it may not be a CIPA requirement, it is an issue that every school should strongly consider addressing in their Internet Safety Policies.)

5. Does CIPA require that school-owned computers used by adults be filtered?

-- Yes, the law explicitly requires all computers be filtered, even those used by adults. Adults can request their computers to be unblocked for bona fide research or another lawful purpose for a specific period of time, but the filtering must be reactivated as soon as they are done.

6. How is 'harmful to minors' defined?

-- CIPA defines "harmful to minors" to mean: any picture, image, 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.

47 U.S.C. § 254(h)(7)(G).

2) A Board-Approved Internet Safety Policy

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.

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.
- The 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) The Education of Minors Related to Online Safety and Cyberbullying (for schools only)

Beginning July 1, 2012, schools must certify that they are educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. Their Internet Safety Policies also must have been updated by July 1, 2012 to reflect their plan to provide the online safety education to minors.

A few important notes:

- At a minimum, the new ISP language should contain this language: "The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response."
- Curriculum can be made to be age appropriate.
- Applicants must keep documentation/records of what you do to comply with the requirement in case of an E-rate audit.
- Unless state law or local policy requires, the updated Internet Safety Policy need not be board approved. However, if you don't have the records of board approval of your *current* Internet Safety Policy (including the policy, board agenda showing there was an opportunity for public comment and the board minutes approving the current policy), you must obtain board approval of the updated policy (making sure the agenda shows an opportunity for public comment before the policy is voted on).

Career & Technology Center Guidance

I received several inquiries from CTCs asking whether they ALSO have to provide the online safety training to students when the students are receiving the training from their 'sending districts' already. After discussing the issue with E-rate program officials, I believe that if your CTC has an agreement with the 'sending district' to provide such online safety education (similar to what you may have already for math or English classes) then you may accurately certify on your E-rate applications that you are CIPA compliant with respect to the online training. However, you should update your ISP to reflect this fact. I am in the process of developing sample "MOU" language that CTCs and sending districts can use for this purpose.

FCC Provides CIPA Clarifications Related to Online Safety/Cyberbullying

In November 2012, the FCC released the answer to 3 CIPA questions related to the education of minors about online safety and cyberbullying. The exact questions and the FCC's answers are below as well as unofficial highlights of the FAQs.

FAQ Highlights:

- Schools must keep records related to the curriculum, trainings and other programs provided to students related to the online safety/cyberbullying training.
- Regular training is required, but annual training is not required. Schools must determine frequency of training based on local needs, and then and specific retain records related to meeting that training frequency.
- Schools are not required to provide education about appropriate online behavior to very young students who are not yet using the Internet in school.
- Schools are expected to train every student and should try to keep records of which students have received training. If a student misses training, the school should take reasonable steps to provide a make-up training or otherwise provide the relevant material to those students.

Q1: What should schools include in their Internet safety policies, and what documents should schools retain to demonstrate compliance with the requirement to educate minors about appropriate online behavior?

A: It is sufficient for a school's Internet safety policy to specify that the school educates its students about appropriate online behavior. A school is not required to provide details about the curriculum, trainings or other educational programs it has chosen in the Internet safety policy itself. Although the FCC does not require schools to specify curriculum in their Internet safety policies, they should keep records of the implementation of their chosen method(s) for educating minors about appropriate online behavior. For example, a school could maintain an annual list of the curriculum, trainings, or other programs provided to its students.

Q2: Are schools receiving E-rate discounts required to provide education about appropriate online behavior to their students every year?

A: The Protecting Children in the 21st Century Act requires a school to certify, as part of its Internet safety policy, that it “is educating minors about appropriate online behavior.” Neither the statute nor the FCC’s rules, however, specify how often a school must provide education regarding appropriate online behavior. While we do not read the statute to require annual trainings, curriculum or online behavior education programs, the phrase “is educating” in the statute suggests some form of regular training. Therefore, schools should determine how frequently they will provide educational programs or curriculum by evaluating local or community needs, and should retain documents demonstrating the frequency with which they provide their students with such programs or access to such curriculum. For example, a school might decide to provide training about appropriate online behavior to its students when they first start using the Internet and then every other year that follows.

Q3: Do schools need to ensure the education of every student in order to be able to certify they are educating minors about appropriate online behavior?

A: Schools should provide education about appropriate online behavior to their students who are actually accessing the Internet using E-rate covered services. Schools are not required to provide education about appropriate online behavior to very young students who are not yet using the Internet in school. Once schools identify the students that should receive education about appropriate online behavior, we expect schools to take reasonable steps to educate these minors. To the extent that a school has a way to record the students that have received training, it may want to retain such records. For example, if a school trains its students using an online education course, it can keep records of which students have taken the online training. Or, if a school educates its students about appropriate online behavior at a school assembly, the school could retain a record of the students in attendance that day. We recognize there may be situations, however, where it would be difficult to demonstrate that all of the students identified as needing the training have been trained, due to student absences or other variables. To the extent a school is aware that some students have missed the scheduled training, the school should take reasonable steps to provide a make-up training or otherwise provide the relevant material to those students.