

What's Next?

Funding Commitment Decisions and Form 486

As we await 2019-20 FCDLs (Funding Commitment Decision Letters) we want to preview our next step in the E-rate application process.

What is the Form 486's purpose?

Applicants are required to file a Form 486 for each Funding Request Number (FRN) that is successfully funded to:

- Notify USAC that services have started for the recipients of service included on one or more FRN.
- Indicate the status of compliance with the [Children's Internet Protection Act \(CIPA\)](#) for the recipients of service for the FRN(s).

Are you CIPA compliant? Can you prove it?

Insufficient Internet Safety Policy makes it to the Top 5 list of [Common Audit Findings](#) in USAC's Schools and Libraries Program.

Every year, on the Form 486, we certify that you are CIPA compliant, but can you prove it? If USAC conducts a Program Quality Assurance audit that requires you produce the following the list below, could you do it?

We've highlighted **Item #3** because, while we believe most of you have #1 and #2 handled, can you verify a Public Meeting was held addressing your district's Internet Safety Policy? Who's in charge of that? As the IT Department head, is it you? We urge you to find out if you're district can truly prove they are CIPA compliant if called upon.

Requirements

CIPA requirements include the following three items:

1. [Internet Safety Policy](#)

Schools and libraries are required to adopt and enforce an internet safety policy that includes a technology protection measure that protects 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. "Minor" is defined as any individual who is under the age of 17.

This internet safety policy must address all of the following:

- 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; and
- Measures designed to restrict minors' access to materials harmful to minors.

For schools, the policy must also include monitoring the online activities of minors. As of July 1, 2012, as part of their CIPA certification, schools also certify that their internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

2. Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters internet access.

The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure 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.

CIPA uses the federal criminal definitions for obscenity and child pornography. The term "harmful to minors" is defined 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 are made by the local community. E-rate Program rules specify that "[a] determination regarding matter inappropriate for minors

shall be made by the school board, local educational agency, library, or other authority responsible for making the determination."

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. For private schools, public notice means notice to their appropriate constituent group.

Additional meetings are not necessary – even if the policy is amended – unless those meetings are required by state or local rules or the policy itself.