



828 West Taft Avenue  
 Orange, CA 92865  
 714-282-6111  
 714-282-6117 Fax  
[www.8e6.com](http://www.8e6.com)

# Complying with CIPA and Keeping Children Safe on the Internet

By The Forsite Group

## Introduction

*The basic goal of CIPA is to protect minors from exposure to online content that's pornographic, obscene, or potentially harmful to them.*

When a convicted child rapist wanted to visit Internet chat rooms under the assumed identity of an 11-year-old girl and surf Web sites featuring pictures of scantily clad children, he didn't have to buy a new computer. As the Pittsburgh Post-Gazette reported, he simply logged on from the library at a local university.

It's the kind of behavior federal legislators had in mind when they wrote the Children's Internet Protection Act (CIPA). The basic goal of CIPA is to protect minors from exposure to online content that's pornographic, obscene, or potentially harmful to them — and from adults who might use communications technology in a potentially harmful way. Though the rapist is back in jail for violating the terms of his probation, his ability to engage in such activity from public computers illustrates the continued challenge for schools and libraries all over the country. Their machines can be used to access inappropriate sites, engage in criminal activity, and even launch hack attacks. That not only jeopardizes the ability of these organizations to comply with CIPA, but also puts their desperately needed federal funds at risk while opening them to legal liability.

One of the keys to ensuring that computers aren't used for such activity — and to complying with CIPA — is to create clear Internet safety and Acceptable Use Policies. The other? Deploy Internet filtering tools that are up to the task at hand.

With its R3000 Internet filtering appliance, 8e6 Technologies helps schools and libraries protect students and minors, remain in compliance with CIPA, and limit their legal liability. It's built especially for educational environments, featuring an extensive database of sites organized into 80 categories, as well as customizable policies that allow adults, minors, and administrators differing levels of access to sites. "Pass-by" filtering makes for fast and scalable performance, while easy installation, setup, and configuration help organizations put it to work right out of the box. And once it's up and running, the R3000 helps schools and libraries guard against the possibility that their computers are used for anything but legitimate and authorized purposes.

## The CIPA Essentials

The tech boom of the 1990s brought easy Internet access not only into the home, but also into libraries and schools. And with it came everything the Internet has to offer — including material many find offensive or harmful to minors. While parents could at least theoretically monitor online content viewed at home, there were no assured protections in public libraries and schools.

*Simply put, CIPA compels libraries and primary and secondary schools to filter out "unwanted" Internet content and address the safety and security of minors using electronic communications.*

Congress took up the issue in 1999, and in December 2000 passed H.R. 4577 — which came to be known as CIPA. Simply put, CIPA compels libraries and primary and secondary schools to filter out "unwanted" Internet content and address the safety and security of minors using electronic communications, including e-mail, chat rooms, and Instant Messaging.

More specifically, CIPA stipulates that schools and libraries certify they have measures in place to block or filter pictures that are obscene, depict child pornography, or are harmful to minors. They must also adopt a policy that specifically addresses the following:

- Access by minors to inappropriate content on the Internet,
- The safety and security of minors when using e-mail 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,
- Access by minors to materials harmful to them.

In early 2001, the Federal Communications Commission (FCC) issued rules to ensure that the provisions of CIPA are carried out. It did so by tying compliance directly to eligibility for E-rate discounts. E-rate is the federal program established in 1998 that awards up to \$2.25 billion per year to help schools and libraries pay for Internet access, internal network connections, and telecommunications. It's subsidized by the small percentage of revenues long-distance providers pay into the Universal Service Fund, which also helps bring phone service to low-income families. As of 2004, there was a total payout of slightly more than \$12 billion in E-rate funding since the program's inception. (E-rate should not be confused with the Enhancing Education Through Technology [EETT] state block-grant program, which is the primary source of federal funding for school technology and which the Federal Government has cut entirely from its proposed 2006 budget.)

Schools and libraries are required to certify they have CIPA measures and policies in place — or are actively working to put them into place — before they can receive E-rate funding for the following year. If they can't, or are later discovered not to have been in compliance by the deadline, they must return whatever E-rate funds they received in that time.

## CIPA In Action

CIPA regulations are comprehensive, but it's also important to note its provisions regarding user privacy and the rights of adults to access the materials they want. For one thing, CIPA does not mandate that Internet activity be tracked and reported — whether it's an adult or a minor who's doing the surfing. For another, CIPA leaves room for adjusting filtering levels according to the user's age — or for disabling filtering and blocking altogether if an adult requests it. (However, even adults cannot ask for filtering to be disabled if they want to view pornography or other obscene material.)

These provisions took center stage when the constitutionality of CIPA was questioned shortly after enactment. The American Library Association (ALA) filed suit, contending that CIPA "induces public libraries to violate the First Amendment by mandating the use of Internet blocking software by adult patrons, children, and even library staff." It also attacked the tie-in to funding,

*As with all issues involving subjective judgments, there is concern over just how individual entities or localities will define "legitimate" online activity or content that's "harmful" to minors.*

arguing that the First Amendment prevents Congress from using funding conditions to "coerce local libraries to adopt a one-size-fits-all scheme far more restrictive than the one most libraries, on their own, would decide to implement."

Initially, a three-judge panel sitting in the Eastern District of Pennsylvania agreed with the ALA's contentions. It held that "CIPA requires plaintiffs to violate the First Amendment rights of their patrons, and accordingly is facially invalid," a ruling that would have permanently enjoined the government from enforcing the act.

But on appeal to the Supreme Court in 2003, the constitutionality of CIPA was upheld. The court found that CIPA does not burden adult library users' access to material "in any significant degree," and that since users can request filters to be turned off, "there is little to this case" on First Amendment grounds; those users can still get access to the sites they want, as long as they ask and as long as those sites are not deemed harmful by library personnel. The court also suggested that if unblocking sites remained too difficult or impeded user access, then patrons would not be prevented from suing the government a second time. Finally, it left open the possibility of evaluating the constitutionality of conditional funding on a case-by-case basis in the future.

In short, as many legal observers point out, the Supreme Court decision essentially confirms the effectiveness and validity of CIPA as a regulation that meets the needs of two major constituents: schools, which understandably want to shield children from potentially harmful content, and public libraries, which just as understandably want to preserve and protect the rights and privacy of patrons engaged in bona fide online research or other legitimate activity.

Still, as with all issues involving subjective judgments, there is concern over just how individual entities or localities will define "legitimate" online activity or content that's "harmful" to minors. Further, CIPA opponents contend that the act is especially unfair to schools and libraries in poorer communities — which don't have the luxury of choosing between compliance and protecting rights if it means losing their main (or only) source of funding.

## Complying with CIPA

Those issues aside, how can schools and libraries be sure they're on the right track when it comes to CIPA compliance? The first step is to establish a clear and comprehensive Internet safety policy. But, since the FCC does not lay out any specific criteria, it's up to individual schools and libraries to formulate their own.

The State E-rate Coordinators Alliance (SECA), which is sponsored by the nonprofit Council of Chief State School Officers (CCSSO), recommends following four practical guidelines in putting together an Internet safety policy:

- Make sure the policy applies to both minors and adults. While CIPA sets out specific requirements regarding children, much of it applies to adult usage as well. Thus, the policy should cover everyone from minors and students to adult patrons and library staff.
- Make sure the policy stipulates the use of an Internet filtering mechanism. That mechanism should, at minimum, block access to the three types of visual content specified in CIPA: obscene material, child pornography, and content considered harmful to minors.
- Make sure the policy emphasizes and assigns staff responsibility in supervising online activity by minors.
- Make sure the policy addresses issues concerning the safe use of e-

***A clear and comprehensive policy is only part of CIPA compliance. After all, blocking or limiting access to harmful content is the key element of the regulation. And for that, a technology solution is required.***

mail and other forms of electronic communication; unauthorized disclosure of personal information; and unlawful online activities.

Those are the most important components of the policy, and they address the basic E-rate requirements. But SECA says that schools and libraries should go the extra step if they want to be sure of properly certifying CIPA compliance. For example, policies should contain a clear statement of objective — perhaps stipulating that access to network and Internet resources will be treated as a privilege. The policy should also make mention of penalties for improper use, and that failure to adhere to policies will subject violators to escalating penalties, from warnings to disciplinary actions to legal proceedings.

Policies should also contain disclaimers on organizational responsibility and privacy, such as "the organization does not warrant the effectiveness of Internet filtering" and "the privacy of system users is limited." Further, there should be provisions governing acceptable use. For example, the policy should cover network etiquette, vandalism and harassment, downloads (music, movies, sound clips), and other issues. Finally, the policy should have special provisions for the use and modification of the organization's own Web site, and it should designate the personnel responsible for specific responsibilities (such as network and user administration).

Of course, if there is already a policy in place, then some common-sense rules apply. Organizations should review it regularly to make sure it applies to the issues they regularly encounter — even if they aren't CIPA-specific, such as student and staff harassment, plagiarism, and copyright violations. Further, they should stay abreast of trends concerning acceptable use; for instance, policies should address usage by adults and not just by students/minors, since the adult-oriented policies common in corporate and government settings are becoming the de facto standard for governing usage in general.

The ALA makes further recommendations for an Internet safety policy. It suggests that schools and libraries post notices at all Internet-access computers, making it clear that use of library equipment to access the illegal materials specified in the Internet use policy is prohibited. Further, organizations should offer a variety of programs at convenient times to educate library users, including parents and children, on the use of the Internet — and publicize them widely. And they should offer users a list of recommended Internet sites, as well as direct links to sites with educational and other types of material best suited to users' needs and interests.

Still, a clear and comprehensive policy is only part of CIPA compliance. After all, blocking or limiting access to harmful content is the key element of the regulation. And for that, a technology solution is required.

## Filtering Facts

Filters are typically deployed at the gateway or aggregation point of the network, where they scan internal traffic headed out to the Internet. If the filter spots a request for an unauthorized site, it sends a block page to the computer from which the request originated, then quickly cancels the session with the site itself. Access is sealed off, and the harmful or inappropriate Web page never loads.

How do filters know when to block a page? They can be programmed with an updatable database of known harmful or unauthorized sites, and they can be set to differing filter levels according to whatever policy is in place.

Filters offer other advantages not specifically related to CIPA. Because they

*Filtering allows organizations to meet the varying needs of their patrons while providing the levels of protection required for CIPA compliance.*

quickly seal off access to unauthorized sites, they minimize the risk of malicious code entering the network — not to mention intruders bent on snooping through systems. They also preserve network performance, since bandwidth isn't consumed in pursuit and download of inappropriate pages or files.

Schools and libraries can select any filtering system that meets the objectives set out in their policies. But simply purchasing and installing a filtering solution doesn't guarantee CIPA compliance. And even if a filtering product is already in place, organizations still might not be in complete compliance.

There are three critical considerations to keep in mind when evaluating a filtering solution for meeting CIPA requirements. First, it must block access to visual depictions of obscenity and child pornography on computers in use by adults. Second, it must block access to visual depictions of obscenity, child pornography, and material harmful to minors when the computer is in use by minors. Third, it must be customizable for both adults and minors, and there must be a way to disable it at the workstation level for adults.

When CIPA was first passed, there were objections over its practical implications — especially concerning the usefulness and accuracy of filtering technology. To some extent, that was true at the time: Filters either over-blocked (that is, limited access to or flagged legitimate sites) or under-blocked (allowed access to the very sites that should have been off-limits). In short, there was no reliable way to ensure which sites were accessible and which weren't — and thus no sure way to comply with CIPA.

A lot has changed in the years since. Advances in filtering technology give organizations much tighter control over the sites they block and the sites they allow access to. Keyword definitions and topic categorizations have been refined and can be cross-referenced against one another much more effectively. Filtering company databases of known harmful sites have grown in size — while at the same time they can be much more easily updated, searched, and customized. Filtering has also become more flexible in general, allowing organizations to meet the varying needs of their patrons while providing the levels of protection required for CIPA compliance.

At the same time, Internet filtering also helps stop bandwidth-wasting activities such as Instant Message (IM) and Peer-to-Peer (P2P) filesharing. Considering that many inappropriate files are pictures, audio or streaming files that require the most bandwidth to access or download, organizations can reduce their IT burden by preserving bandwidth through Internet filtering. Search engine images, for example, pose risks to schools and libraries. Many filtering solutions are unable to block inappropriate images, which leaves these solutions obsolete. Students have quickly learned to bypass many filtering solutions, exposing themselves and others to inappropriate images and other Web content. This leaves schools and libraries as vulnerable as if they had never had a filtering solution in the first place.

## How 8e6 Aids CIPA Compliance

8e6 Technologies has taken the lead in helping schools and libraries meet the requirements outlined in CIPA. Since 1995, it has been one of the top suppliers of Internet filtering and reporting technology for thousands of organizations across the United States, at the district, county, and state levels (Arkansas, Rhode Island, West Virginia, and Wisconsin are among the states that have adopted the 8e6 filtering solution).

With the R3000 Internet filtering appliance, 8e6 specifically addresses the needs of schools and libraries. It offers a range of critical features that can help

*The R3000 imposes no performance penalty. It's a standalone device that sits outside the flow of network traffic, where it "watches" Web site requests instead of stopping them to make its assessment.*

in protecting minors from harmful content while helping organizations limit their own legal liability and meet the compliance requirements set out in CIPA:

- A comprehensive, human-verified URL database broken out into 80 categories — sorted by everything from "alcohol" and "games" to "child pornography" and "weapons"—which gives organizations an accurate and selective solution for filtering and monitoring.
- Instant Messaging (IM) and Peer-to-Peer (P2P) blocking, which keeps users from accessing and sharing media files that not only might be harmful to minors — but also could harbor malicious code and consume bandwidth.
- Real-time probes that allow administrators to keep a close eye on a user's Internet activity and ensure it remains lawful and appropriate. Reports generated by the probes can be exchanged via e-mail when further review is warranted.
- "X-Strikes" blocking, which lets administrators set criteria for automatically restricting a computer's Internet access after a predetermined amount of attempts to view inappropriate Web sites has been made.
- Google SafeSearch enforcement, which blocks access to inappropriate content within the Google search engine — including images.
- User group profiles, which allow varying levels of access to be set up depending on job title, rights, or other criteria.
- Time-based filtering, which gives organizations greater flexibility over when certain sites can be accessed.
- A Customer Feedback Module (CFM) that enables automatic database updates. The CFM is an auto-learning feature that sends the most frequently visited uncategorized URLs from participating customers back to 8e6 on a daily basis; the selected URLs are then reviewed and added to one of 8e6's 80 database categories.

But there's more to the R3000 than its CIPA-specific features. There are filter models available for different network environments, including the R3000G for up to approximately 30,000 workstations/users and the R3000MSA for small to mid-size educational environments with up to 2,500 workstations/users. Also available is the Enterprise Reporter 3.0, which works in conjunction with the R3000 filter and provides detailed reports on Internet usage without compromising filtering speed and performance, or any other server/network functions. The Enterprise Reporter is built on a robust and stable operating system based on Red Hat Linux and features remote and multi-level administration. Further, both the Enterprise Reporter and the R3000 are easy to set up, install and configure.

Equally important, the R3000 imposes no performance penalty. It's a standalone device that sits outside the flow of network traffic, where it "watches" Web site requests instead of stopping them to make its assessment. This "pass-by" filtering is much more efficient than "pass-through" filtering, which slows the flow of data and can even create a choke point if traffic exceeds certain levels. In short, the R3000 keeps packets moving, even in heavy traffic situations, without creating a point of failure.

And education customers are proving more than satisfied with the 8e6 solution. "Performance has exceeded all of our expectations," says David Ferris, client liaison with Miami-Dade County Public Schools, which has more than 60,000 users.

## Conclusion

*Clear and comprehensive Internet safety and acceptable use policies are the first step in meeting the requirements set out in CIPA.*

CIPA compliance is an ongoing challenge for schools, libraries, and other organizations whose computers can be used for activity potentially harmful to minors. At risk is not only the safety of students — but also the E-rate funds that many organizations rely on to offer Internet connectivity and maintain the necessary infrastructure.

Clear and comprehensive Internet safety and acceptable use policies are the first step in meeting the requirements set out in CIPA. But regardless of their policies, schools and libraries must also implement filtering technology that specifically addresses the law's provisions. With its R3000 Internet filtering appliance, 8e6 Technologies furnishes the solution these organizations need. Thanks to 8e6, schools and libraries can preserve the funds they rely on-and protect the users whose safety they're entrusted with.



For more information on 8e6 Technologies and 8e6 appliance-based solutions for Internet Filtering, Web-use Reporting, and Spam Control, visit [www.8e6.com](http://www.8e6.com).