CIPA Compliance
Keeping Kids Safe on the Web

Contents

Introduction

The Children's Internet Protection Act (CIPA) is a federal law passed by Congress in 2000, and updated and clarified since, to help ensure the safety of children accessing the Internet over school and library computers. The act requires schools and libraries to use filtering to block dangerous or offensive material from minor users.

Any organizations that receive funding through E-Rate or the Universal Service Fund must certify that they are meeting the requirements of CIPA.

What CIPA Requires

Any organization included under the CIPA guidelines must meet the following four criteria: A Technology Protection Measure, An Internet Safety Policy, an education program, and a policy to monitor the online activities of minors. [i]

Utilize a Technology Protection Measure.

A Technology Protection Measure is defined as: "a specific technology that blocks or filters Internet access to visual depictions that are— (A) obscene (B) child pornography; or (C) harmful to minors." [ii]

The term "harmful to minors" is further defined as:

> "Any picture, image, graphic image file, or other visual depiction that-- (A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (B) 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 (C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors." [iii]

Filtering is required on all computers, whether used by adults or minors. However, the filtering may be disabled for adult users when requested.

Create and enforce an Internet Safety Policy.

This required policy must address:

- Access by minors to inappropriate matter on the Internet

- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications

- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online

- Unauthorized disclosure, use, and dissemination of personal information regarding minors

- Restricting minors' access to materials harmful to them [iv]

Monitor online activities of minors
Schools must also adopt and enforce a policy to monitor the online activities of minors.

Education program
Schools and libraries must also certify that minors are being educated about appropriate online behavior. This should include information about cyberbullying, the sharing of personal information, and online communication.

An update to CIPA in 2011 requires that schools change their Internet Safety Policy to include teaching about online behavior and social networking.

> The rule is:
>
> "Internet safety policy must provide for 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."

Changes must be in place July 1, 2012.

10 Facts about CIPA and Web Filtering

Blocking inappropriate content doesn't have to block learning
The Children's Internet Protection Act (CIPA) is a federal law passed by Congress in 2000, and updated and clarified since, to help ensure the safety of children accessing the Internet over school and library computers. Any organizations that receive funding through E-Rate or the Universal Service Fund must certify that they are meeting the requirements of CIPA.

1. CIPA requires a web filter for schools that receive E-Rate funding.

2. CIPA requires that schools block visual depictions that are pornographic, obscene, or harmful to minors.

3. CIPA requires a policy for educating users, including educating minors about appropriate online behavior and interacting with other individuals on social networking sites; a policy for Internet Safety; and monitoring the activity of minors.

4. CIPA requires filtering on school-owned devices (even mobile devices); clarification on requirements for student-owned devices used on campuses is forthcoming from the FCC.

5. Allowing YouTube videos is not a violation of CIPA.

6. Allowing social networking is not a violation of CIPA.

7. Schools won't lose E-Rate funding for adjusting filtering policies to unblock appropriate sites.

8. While teacher computers need to have a web filter installed, teachers and other adults don't need to be filtered (i.e., the ability for adults to override the filter is not a CIPA violation).

9. Schools have the authority to make local decisions about filtering policies.

10. Even the FCC recognizes the necessity and benefits of teaching students to be responsible digital citizens.

Straight from the DOE: http://mindshift.kqed.org/2011/04/straight-from-the-doe-facts-about-blocking-sites-in-schools/

FCC Report: http://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0819/FCC-11-125A1.pdf

Content Filtering with the Lightspeed Systems Web Filter

Content filtering is a primary feature of CIPA, as well as most school Acceptable Use Policies outlining web browsing behavior. Content filtering allows schools to block content that is dangerous or inappropriate for minors.

The Lightspeed Systems Web Filter ensures that users' web browsing is in line with CIPA mandates as well as Acceptable Use Policies—while they are on the network or when utilizing school computers off the network. Our education-specific database is comprehensive and accurate, ensuring that inappropriate sites are no longer a click away, but that valuable content remains available to users.

The Web Filter detects and/or blocks access to inappropriate material on the Internet based on our extensive, education-specific URL database with more than one billion entries, as well as your own custom allow and block lists. Our content filter groups sites into about 120 school-specific categories based on subject matter and age-appropriateness, providing easy review and administration.

Students bypassing a school's Internet filter is a great concern, for maintaining student safety as well as CIPA compliance. As proxy technology becomes more complex in attempts to anonymously tunnel users through content filters, Lightspeed Systems continues to develop new proxy-blocking methods. By blocking secure, unsecure, and anonymous proxies, you can ensure that Acceptable Use Polices are enforced and CIPA compliance is maintained.

Secure – Block users using HTTPS sites to bypass your content filter. When using the HTTPS protocol, it encrypts the data that the person is trying to access, making

it difficult for other filters to block those types of sites. With the Lightspeed Web Filter, you can end this battle by blocking secure proxies.

Unsecure and Anonymous – Block users accessing HTTP sites which, though not encrypted in any way, may be inappropriate. With the Lightspeed Web Filter, you can block unknown URLs, domains and IP addresses of known proxies, unknown URLs that match proxy patterns, and all proxied requests.

The flexible configuration and customization of the Lightspeed Web Filter allow you to accommodate different groups of users as well as your own specific policies while ensuring compliance and safety. This ensures that neither over-blocking nor under-blocking hinder the usefulness of your network for education, while keeping browsing behavior in line with Acceptable Use Policies and CIPA mandates.

While we have a room full of servers scouring the Web for inappropriate sites, we also have a team of dedicated live people who ensure accuracy, review questionable sites, and promptly respond to customers with questions or requests regarding our categorization and blocking of specific web sites.

CIPA Compliance with the Lightspeed Systems Web Filter

The Lightspeed Systems Web Filter provides the necessary support for compliance with the specifications detailed in CIPA with comprehensive web filtering controls and user activity reporting.

CIPA Requirement	Web Filter Feature
Specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.	Comprehensive and accurate education-friendly URL database with more than one billion entries, allowing you to: • Block web sites categorized as containing adult and pornographic subject matter • Block web sites categorized as promoting the use illicit or illegal drugs • Block web sites categorized as promoting violence, hate, weapons, alcohol, and gambling. • Block web sites categorized as containing unmoderated forums, instant messaging services, web mail services, chat and dating services, as well as personal and social networking services. • Block web sites promoting and/or supporting illicit and illegal network intrusion and infiltration • Block web search queries that use blocked content category keywords • Enforce 'Safe Search' search engine options • Block the display of blocked category web site images • Block access to unknown/uncategorized web sites Multiple layers of secure, unsecure, and anonymous proxy detection and blocking to keep users from bypassing your filter and accessing blocked sites Daily signature updates, and immediate emergency updates, directly from Lightspeed Systems

Filtering on all school computers.	Guide Mobile Filter provides filtering protection for mobile users utilizing school computers outside the network—without a VPN, from any location with any type of Internet connection
Ability to turn off filtering for adult use.	Access differentiation by user, IP, group, organizational unit, domain
Monitor online activities of minors.	Comprehensive reporting on user behavior, from a high-level overview to detailed reports on individual user activity, including: • Internet traffic activity by content category • URLs visited • Blocked Internet requests by content category • All search engine queries • Blocked search engine queries • Suspicious queries • Unknown/uncategorized URLs • Overrides (active and history)
Teach students about appropriate online behavior	My Big Campus provides a safe, social learning environment, as well as lessons and resources about digital citizenship, netiquette, and online safety.

Balancing Safety and Education

A 2003 study by the Department of Commerce and National Telecommunications and Information Administration investigated how well available Technology Protection Measures met the needs of schools. In their study, they identify several needs of educational institutions beyond simply blocking inappropriate content. Among those are:

> Balancing the importance of allowing children to use the Internet with the importance of protecting children from inappropriate material

> Accessing online educational materials with a minimum level of relevant content being blocked [v]

Lightspeed Systems recognizes this need to balance safety and education, and the importance of not over-blocking valuable content. To this end, we offer innovative features to make Web 2.0 content safe and compliant; the ability to create custom allow and block lists; and the ability to customize filtering profiles for different users, different ages, special projects, and more.

My Big Campus, a social learning management system (LMS), provides a safe, monitored environment for students and teachers to collaborate, communicate, and learn.

CIPA Compliance in the Age of Mobility

CIPA requires filtering for school-owned mobile devices on campus. The FCC has stated that they will clarify requirements for school-owned devices off campus and student-owned devices on campus. Even aside from CIPA requirements, though, content filtering on mobile devices provides security and peace of mind to districts—and Lightspeed Systems solutions can help.

Our Web Filter offers cross-platform filtering on mobile devices to extend the safety to mobile users, with on- and off-network filtering and policy enforcement available for iOS, Android, Win 8 and other handheld devices; as well as MacBooks, laptops, and netbooks.

And our Mobile Manager MDM solution provides the ability to block explicit content in the iBook store and iTunes store; as well as set a maximum rating for downloaded shows and movies.

Lightspeed Systems is committed to helping schools create safe, collaborative, mobile learning environments through our solutions. Finding a balance between learning and safety is integral to this mission, and we will continue to develop solutions to help ensure that the safety of your students and security of your network don't limit the educational potential of the Internet, and that the power of the Internet doesn't compromise the safety of your students or the functions of your network.

Conclusion

The Internet offers valuable benefits—but is also full of content that can be harmful to minors. To comply with CIPA regulations and Acceptable Use Policies, you have to ensure that students are protected from potentially dangerous and inappropriate content. The Lightspeed Web Filter provides comprehensive, customizable filtering as well as innovative features for collaboration and mobility to ensure web browsing and searching are safe and appropriate so you can meet CIPA compliance.

For More Information

E-Rate: http://www.e-ratecentral.com/CIPA/Childrens_Internet_Protection_Act.pdf

FCC: http://www.fcc.gov/cgb/consumerfacts/cipa.html

CIPA FAQ: http://www.sl.universalservice.org/reference/cipafaq.asp

FCC Consumer Factsheet: http://www.fcc.gov/cgb/consumerfacts/cipa.pdf

About Lightspeed Systems

Lightspeed Systems solutions transform learning by safely and easily connecting people, resources and technology. Since 1999 we've partnered with thousands of school districts to protect and engage millions of students. www.lightspeedsystems.com

---

[i] http://www.e-ratecentral.com/CIPA/Childrens_Internet_Protection_Act.pdf
[ii] http://www.e-ratecentral.com/CIPA/Childrens_Internet_Protection_Act.pdf
[iii] http://www.e-ratecentral.com/CIPA/Childrens_Internet_Protection_Act.pdf
[iv] http://www.fcc.gov/cgb/consumerfacts/cipa.html
[v] http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/cipareport_08142003.html