WHITE PAPER:

Managed Security: A Guide to Understanding The Children's Internet Protection Act (CIPA)

The Internet is a great and powerful tool and provides users access to volumes of information on virtually any topic. It makes doing research quick and easy and can be used as an important learning tool for children. Unfortunately, it can also be misused and children can too easily locate undesirable information that could be harmful to minors and put them at risk and make them vulnerable to dangerous people. The White Paper has been written to provide you with information on a federal law enacted by Congress to address these concerns.

TeamLogicIT®
Your Technology Advisor

Introduction

"The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program — a program that makes certain communications technology more affordable for eligible schools and libraries."[1]

Although TeamLogic IT can play a central role in helping schools and libraries comply with CIPA, fulfilling the obligations of CIPA cannot be achieved by technology alone. Rather, it requires the combination of:

- Technology Protection Measures
- Internet Safety Policy
  - — Enforcement
  - — Education
  - — Monitoring (for schools)
- **Certification**

This document is intended to breakdown the complexities of CIPA and guide readers in making informed decisions to achieve compliance. *Disclaimer: TeamLogic IT does not offer legal advice and cannot guarantee the accuracy of this document. You should consult with an attorney whenever you think it necessary.*

1. Technology Protection Measure

The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions (thus it does not apply to text) that are:

- **Obscene**, as that term is defined in section 1460 of title 18, United States Code;
- **Child pornography**, as that term is defined in section 2256 of title 18, United States Code; or
- **Harmful to minors** (for computers that are accessed by minors, under 17 years of age). Defined as any picture, image, graphic image file, or other visual depiction that:
  - — Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
  - — 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
  - — Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

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

The protection is not required to be 100% effective, which would be an impossible standard, and the FCC has declined to define or specify any such measures or targets.

"We have attempted to craft our rules in the most practical way possible, while providing schools and libraries with maximum flexibility in determining the best approach. We conclude that local authorities are best situated to choose which technology measures will be most appropriate for their relevant communities."
— FCC regulations, April 2001

"We decline to follow the suggestions of commenter's to incorporate within our regulations layman's explanations of obscenity, child pornography, and the term "harmful to minors." We decline to amplify the statutory definitions."
— FCC regulations, April 2001

2. INTERNET SAFETY POLICY

The adoption of an "Internet Safety Policy" that addresses:

- Technology protection measures (mentioned above.)
- Access by minors to inappropriate matter, as determined by the school board, library board or administration.
- 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 (as defined above in Technology Protection Measure.)
- Educating minors of appropriate online behavior, including cyber-bullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.
- For schools only, a policy to monitor online activities of minors. This does not include the actual online tracking of Internet use by minors or adults.

Prior to adopting the Internet Safety Policy, CIPA requires reasonable public notice and at least one public hearing or meeting to address the proposed policy.

3. CERTIFICATION

There is no such thing as a CIPA-certified product, and no vendor should make that claim. For the purpose of CIPA,

- Certifications for schools eligible for E-rate discounts may be made by the relevant school, school board, local educational agency, or other authority with responsibility for administration of the school (the Administrative Authority.)
- Certifications for libraries eligible for E-rate discounts may be made by the relevant library, library board, or other authority with responsibility for administration of the library (the Administrative Authority.)
- Certifications are made either on FCC Form 479 or FCC Form 486 depending on whether the Administrative Authority is also the Billed Entity.[2]

"Some commenter's have requested we require entities to certify to the effectiveness of their technology protection measures. Adding an effectiveness standard does not comport with our goal of minimizing the burden we place on schools and libraries. Therefore, we will not adopt an effectiveness certification requirement."
— FCC regulations, April 2001

OTHER CONSIDERATIONS

CIPA addresses a subset of what most schools and libraries consider acceptable use of their networks. Schools and libraries may choose to filter content and applications beyond the specified visual depictions in CIPA. Libraries, however, may expose themselves to legal challenges based on the blocking of constitutionally protected content and must weigh these concerns. Nevertheless, schools and libraries need to protect their computers and networks against viruses, spyware, and other malware by filtering for these threats on all open protocols: HTTP, FTP, SMTP, POP, IMAP, etc.

- The Virginia Department of Education has posted "Acceptable Use Policies: A Handbook" at: http://www.doe.virginia.gov/VDOE/Technology/AUP/home.shtml.
- The handbook lists the elements of an Acceptable Use Policies appropriate for schools as well as multiple samples and template, including student agreement and parental permission forms.

CIPA makes no distinction between computers used only by staff and those accessible to the public. The requirements, therefore, apply to all computers with Internet access. CIPA requires that the school or library be able to easily disable filtering for an adult to enable access for bona fide research or other lawful purposes.

2. http://www.sl.universalservice.org/reference/CIPAfaq.asp

References

FCC Consumer Fact Sheet on CIPA
http://www.fcc.gov/cgb/consumerfacts/cipa.html
USAC Discussion of CIPA Requirement
http://www.usac.org/sl/applicants/step10/cipa.aspx
USAC CIPA FAQ
http://www.sl.universalservice.org/reference/CIPAfaq.asp
Full CIPA Text
http://ifea.net/cipa.html
CIPA: A Brief FAQ on Public Library Compliance by Wisconsin Department of Public InstructionCIPA
http://dpi.wi.gov/pld/cipafaqlite.html

About TeamLogic IT Managed Security Offering

TeamLogic IT Managed Security enables schools and libraries to keep their students safe while on the Internet and focused on learning. In particular, We can assist schools and libraries in:

- Keeping inappropriate content out of the classroom and computer lab
- Creating a safe learning environment
- Achieving CIPA compliance
- Qualify for E-Rate funding
- Protecting computers from spyware, viruses, and other malware
- Our Managed Security graphical user interface and virtual rack metaphor makes it is easy for school and library staff to administer.

For help with Managed Security, contact your local TeamLogic IT office.

TeamLogic IT is a national provider of advanced IT management services for businesses. With locations across the U.S., TeamLogic IT provides managed services, computer consulting and support services focused on helping companies minimize downtime and improve productivity. TeamLogic IT helps businesses compete better through the effective use of information technology.

APPENDIX: CIPA AND THE TEAMLOGIC IT EDUCATION PACKAGE

CIPA Requirement	How TeamLogic IT Education Package Can Help
Technology Protection Measure	Filter web content by 53 categories including Pornography/Sex, Nudity, and Proxy/Anonymizer sites that may be used to circumvent simpler filters
Access by minors to inappropriate matter	Filter web content by 53 categories including Mature, Violence, Hate Speech, Illegal Drugs, Dating, and more
The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications	Restrict access to web mail, chat/IM by sites and port hopping IM applications or protocols
Unauthorized access, including so-called "hacking," and other unlawful activities by minors online	Filter criminal/hacking sites to prevent minors from learning these skills and downloading hacking tools
~~**Monitoring of minors**~~	Reports allow for monitoring web usage and policy violations, including reports by Active Directory user name.
~~**Policy controls** to provide different policies for~~ adults and minors	Define different filtering policies, such as staff, teacher, and student, by: Computer Active Directory User Time of Day