

The Children's Internet Protection Act (CIPA)...

Complying with the Old
and the New

Presented by:
Julie Tritt Schell
PA E-rate Coordinator
May 2012

Overview

- Recap of Original CIPA Requirements
- Details of New CIPA Requirements
- CIPA Clarifications
- Filtering Update for New Technologies



First, the original...

Recap of Original CIPA Requirements

- Children's Internet Protection Act (CIPA) requires schools and libraries to:
 - Have a board-approved Internet Safety Policy
 - Filter Internet access from certain visual depictions
 - Monitor online activities of students (schools only)
- Applies to schools and libraries receiving Internet access and internal connections services
 - Does not apply if only receiving discounts on telecommunications services
 - If a school or library is in an Internet consortium, they still must be CIPA compliant

Original CIPA: Internet Safety Policies

- Must be approved by governing board after a public hearing or open meeting for which reasonable notice is provided
 - For private schools, “public” notice means notice to their appropriate constituent group
 - For public schools, a meeting where public comment is permitted satisfies the public hearing requirement
- Must address:
 - Access by minors to inappropriate matter
 - Safety/security of minors when using e-mail, chat rooms, other 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

Original CIPA: Technology Protection Measures

- Schools and libraries must use specific technology that blocks or filters Internet access
 - Filter can be set to different levels, depending on age of user
- Must protect against access by adults and minors to visual depictions that are obscene, child pornography, or harmful to minors
- Applies to all computers, not just computers used by students
- May be disabled for adults engaged in bona fide research or other lawful purposes
 - Note, there are no provisions to disengage filter for students
 - Filter cannot be permanently disabled for adults

Harmful to Minors Defined As....

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).

Original CIPA: What To Keep

- Copy of approved policy
- Notice of public hearing or public meeting (such as school board meeting) where CIPA policy was considered and voted upon
 - Agenda for meeting – show opportunity for public input/comment before adoption of CIPA policy
 - Other documentation for opportunity for public comment
- Filtering records, purchase orders
- Method for monitoring online activity of students
- Information does not get submitted to PDE or USAC, but must be retained and provided upon request

Original CIPA: How Long To Keep

- Schools must retain their Internet Safety Policy documentation for at least five years after the last date of service for a particular funding year
 - For example, if a school held a public hearing and adopted its Internet Safety Policy in 2001 and relied on that same policy to make its Form 486 CIPA certification in FY 2011, the school must retain its Internet safety policy documentation (from 2001) for five years after the last day of service for FY 2011, which would be until June 30, 2016.
- If you don't have this documentation, you should issue a new public notice, hold a new public hearing, and adopt your current Internet Safety Policy to become compliant
- No CIPA violation has occurred if the hearing or meeting was held prior to August 2004 and records of the notice and the hearing or meeting cannot be produced



And now, the new...

New CIPA Requirements

- Beginning July 1, 2012, schools' Internet Safety Policies must address:
 - *Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms*
 - *Cyberbullying awareness and response*
- This means that schools are required to teach online safety to students as a prerequisite to receiving E-rate funding beginning with the 2012 school year
 - Public libraries are not included

Internet Safety Policies

- Internet safety policy must be updated by July 1, 2012
 - New public hearing not required
 - But board must approve change to policy if required under local policies
 - If such board approval is required, it must be done before July 1, 2012.
- Policy cannot say that the school “may” educate students
- District’s cyberbullying policy alone is not sufficient unless it addresses all the required elements

CTC and IUs with Part-Time Students

- Several CTCs have asked 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
- This would presumably apply to IUs with part-time students as well
- CTCs should update their ISPs to reflect the fact that the training will be done by the 'sending district'
- Suggestion: Enter into a MOU with each sending district so the CTC/IU has appropriate documentation

Sample ISP Language

- Minimal 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.*
- More comprehensive language:
 - *Students are required to complete an Internet safety course. The curriculum focuses on educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The course consists of an interactive presentation and will be completed prior to the end of the first semester of the school year. Students enrolling after the first semester are required to participate individually with a designated presenter. All students in grades 3-12 will sign a verification form indicating they have participated in the course. Students in grades K-2 will not be required to sign off, but the designated presenter will list the names of those who complete the K-2 instruction. (Erie City School District)*
 - Entire District AUP:
http://www.eriesd.org/ecsd/media/files/pdf/AUP_Student.pdf

Sample ISP Language

- *From the Upper Moreland Township's ISP:*
 - *Internet Safety shall be a component of the district's standards-based Business, Technology Education, and K-12 Library curriculum to include instruction regarding but not limited to appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.*
- The Butler Area School District's ISP is also very good:
 - http://www.psba.org/districts_policies/b/80/POLBUTL815.pdf.
- The Penn Manor School District's 1-page Internet Safety Policy is a great model for a concise, compliant policy:
 - <http://www.pennmanor.net/techblog/wp-content/uploads/2010/08/iSafetyPolicy2010.pdf>.

Online Safety Education Resources

- Just as important as having your ISP updated to be CIPA compliant is the actual cyber safety training that must begin with the 2012 school year
 - Since it's part of curriculum, teachers and administrators should assist in the development of curriculum and implementation plan
 - The plan can be tailored to the age and maturity of the students. What is taught to 1st graders will be different from what is taught to HS seniors
- **Are all students required to receiving CIPA training every year? *****
 - **Despite earlier advice, FCC staff now consider this an 'open issue.'**
- Key is to develop an implementation plan and document compliance with the plan
- Two resources that may be of assistance:
 - The Northern York County School District has developed an Internet Safety and Cyberbullying Implementation Plan for each grade which is particularly well done (handout)
 - West Virginia also has developed a Cyber Safety Curriculum example for each grade (handout)

Online Safety Education Resources

- Carnegie Mellon University: <http://www.carnegiecyberacademy.com>
 - Great free resource for 4th and 5th graders!
- Common Sense Media:
<http://www.common Sense Media.org/educators/curriculum>
<http://www.common Sense Media.org/educators/erate>
 - Free toolkit with great training resources to become CIPA compliant
- National PTA Association: http://www.pta.org/topic_internet_safety.asp
- The National Center for Missing and Exploited Children:
<http://www.nsteens.org/TeachingMaterials> and <http://www.netsmartz.org/Educators>
- The National Criminal Justice Reference Service:
<https://www.ncjrs.gov/internetsafety>
- iSafe: a PAIUnet partner that provides Internet Safety Curriculum to schools

iSafe/PAIUnet Partnership

- Content was provided free to schools for 2011 through the PAIUnet Statewide Act 183 Grant
- Schools that are PAIUnet members may purchase iSafe at a rate of \$.20 per student per year for the 2012 and 2013 school years
 - To subscribe, go to the Keystone Catalog (<http://keystonecatalog.paiunet.org/>) to place your order. You will then be contacted with further instructions
 - Questions? Send an email to paiunet@isafe.org

NEW CIPA Documentation

- In addition to all original CIPA documentation, the following should be kept to demonstrate NEW CIPA compliance:
 - Documentation of cyberbullying/appropriate online behavior education for all minors
 - Could be curriculum, sign-in sheets, teacher lesson plans, etc.
 - Keep records of when education occurred, to whom
 - Updated Internet Safety Policy, with approval date before July 1, 2012



CIPA Clarifications and BYOD Issues...

CIPA Clarifications

- Local school and library authorities must determine what matter is inappropriate for minors
- Specific social networking sites are not automatically considered “harmful to minors” or assumed to fall into one of the categories that schools or libraries must block
 - The FCC specifically noted that Facebook or MySpace are not required to be blocked under FCC rules
- Although the FCC rules talk about Internet Safety Policies, it doesn’t matter what the name of your actual policy is, as long as it contains the required elements and was approved by your board as an official school policy

Filtering Update for New Technologies

- FCC acknowledged that current rules may not address the filtering requirements when personal computers and devices are brought to school and will soon request public comment
 - When the FCC requests public comment, I encourage you to participate
- Based on informal conversations, we believe:
 - Any school-owned computer/device must be filtered, whether it is used on campus or off, or used by an adult or student
 - Any personal-owned computer/device must be filtered if using school or library Internet access
 - May not be required: Personal-owned computer/devices that use their own Internet access
 - Be careful with this. Just because it's not required, doesn't mean you shouldn't address it!
- As of now, no exceptions for cellular devices

Filtering Requirements: When and Where?

- School-owned devices used at school:
 - The law is clear that all school/library owned computers need to be filtered at school
 - Last year the FCC verbally clarified that computers includes all devices with Internet access (including portable ones)
- School-owned devices used off-campus:
 - 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.
 - In 2011 the FCC verbally stated that school owned computers used off campus must be filtered
 - In late April 2012, FCC stated that issue is still ‘open’ and has not been decided

Filtering and BYOD Initiatives

- Privately-owned devices used at school, using school's Internet:
 - FCC acknowledged in August 2011 CIPA Order that current rules may not address the filtering requirements when personal computers and devices are brought to school

“Some E-rate recipients have sought guidance regarding the potential application of CIPA requirements to the use of portable devices owned by students and library patrons, such as laptops and cellular telephones, when those devices are used in a school or library to obtain Internet access that has been funded by E-rate. We recognize that this is an increasingly important issue, as portable Internet access devices proliferate in schools and libraries. We believe it may be helpful to clarify the appropriate policies in this area, and intend to seek public comment in a separate proceeding.”

- **When this proceeding is initiated, I encourage you to file comments**
- Because FCC acknowledged that this is an ‘open’ issue, it should be difficult for FCC to recover E-rate funding for current procedures that do not require filtering of privately-devices used on-campus

Filtering and BYOD Initiatives

- Privately-owned devices used on campus, using private Internet access (such as 3G, aircards)
 - This also is an open issue, but less likely a CIPA issue if not using a school device or school Internet
 - However, you should be sure your ISP addresses the appropriate use of these devices (and perhaps filtering) regardless of whether CIPA requires it
- *As of now, no exceptions for cellular devices*

Advice:

Do your absolute best to comply with the spirit of CIPA through policy and practice. If you are filtering all devices the best you can and protecting your students from visual depictions that are obscene, pornographic, or harmful to minors, the FCC should take this into consideration if you are ever audited.

Questions?

To join the PA E-rate Listserve, send an e-mail to:

jtschell@comcast.net

Include your name and school (or library) name