Digital Learning Environments Series
Vol. 1, No. 1

A Brief on Internet Safety and E-rate Compliance with the Children's Internet Protection Act (CIPA) the Neighborhood Children's Internet Protection Act (NCIPA) and the Broadband Data Improvement Act (BDIA) (a.k.a. The Protecting Children in the 21st Century Act)

(http://www.ncpublicschools.org/docs/erate/training/cipa-faq.pdf)

May 26, 2010

North Carolina Department of Public Instruction
Instructional Technology/Connectivity Services

This brief is divided into the following areas:

Adapted May 26, 2010 with permission from R. Bocher and Wisconsin Department of Public Instruction (2004), *FAQ on E-rate Compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act*.

Disclaimer: While reasonable efforts have been made to ensure the accuracy of this information, only information from the Federal Communications Commission (FCC) or the Schools and Libraries Division (SLD) should be considered official. On November 5, 2009, the FCC released a Notice of Proposed Rule Making (NPRM) FCC 09-96 to propose revising the FCC rules regarding the E-rate program to comply with the requirements of the Protecting Children in the 21st Century Act. Comments on the NPRM were due to the FCC on or before February 18, 2010, and reply comments on or before March 5, 2010. For information on how to file comments, refer to Public Notice DA 10-102. If applying for E-rate funding beyond what the FCC defines as basic telecommunications services schools must consider any policy, procedure, or project in relation to current and future FCC rules related to CIPA. The following is intended to help schools identify circumstances in order to determine if any actions are needed. School boards should consult counsel familiar with FCC rules and judicial interpretation regarding CIPA in order to craft appropriate policy and procedures related to implementing "Internet Safety Policy" and "Technology Protection Measure" requirements. In addition, school boards would be well advised to provide for an opportunity for public input before adopting revisions to their "Internet Safety Policy" and "Technology Protection Measure", consistent with the original CIPA statutory requirements.

Note: On May 20, 2010, the FCC released a Notice of Proposed Rule Making (NPRM) FCC 10-83 to propose revising the E-rate program to support the goals of the National Broadband Plan and to cut red tape. In this seminal NPRM the FCC requests comments on a number of significant changes to the E-rate program. Two potential changes could impact CIPA compliance. 1. The FCC proposes: "to adopt the National Broadband Plan recommendation to provide full E-rate support for wireless Internet access service used with ~~a~~ portable learning devices that are used off premises." Current rules require any "at home" use to be cost allocated. Conceivably, the current CIPA rules would apply to the eligible service regardless of location; hence the requirement to filter any of "its" computers with Internet access would thus apply. In addition, the NPRM seeks comment regarding the need for additional local policy requirements related to this potential rule change. 2. The FCC seeks comment: "on whether we should allow schools that serve unique populations to receive E-rate funding for priority one and priority two services delivered to residential areas. Conceivably, the current CIPA rules would apply to the eligible service regardless of location; hence the requirement to filter any of "its" computers with Internet access would thus apply.

Schools have always had wide latitude when it comes to implementing Internet safety curriculum, policy and protection measures...

"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

1. Background

The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA) passed Congress in December of 2000. Both were part of a large federal appropriations measure (PL 106-554). The Federal Communications Commission released its regulations for CIPA and NCIPA covering the E-rate program in April 2001. See the Sources section at the end of this document for references to the Commission's regulations and more information on this legislation.

CIPA and NCIPA: There is some overlap in language between these two sections of PL 106-554 but they do address different areas. The Children's Internet Protection Act addresses what has to be filtered and the need for an Internet safety policy. The Neighborhood Children's Internet Protection Act focuses on what has to be included in a school or library's Internet safety policy. Moreover, NCIPA is applicable only to the E-rate program.

BDIA: The Broadband Data Improvement Act (BDIA), often referred to as the Protecting Children in the 21st Century Act, enacted October 10, 2008, added language requiring school districts receiving E-rate discounts on Internet Access and Internal Connections to educate students about appropriate behavior on social networking and chat room Web sites, as well as the dangers of cyber bullying.

Federal programs: CIPA compliance is required when using funds for particular purposes from three federal programs: E-rate, ESEA Title II D (Ed Tech), and LSTA. When a school or library receives discounts from the E-rate program, its CIPA requirements take precedence over the requirements in the ESEA or LSTA sections of CIPA.

Previous Congressional actions on filtering: CIPA was not the first attempt by Congress to regulate Internet content or Internet access. The Communications Decency Act (CDA) was part of the Telecommunications Act of 1996, the same act that included the E-rate program. The CDA was subject to an immediate lawsuit and was ultimately found unconstitutional on First Amendment grounds by the Supreme Court in 1997. Following failure of the CDA to pass constitutional muster, Congress passed the Child Online Protection Act (COPA) in October 1998 (not to be confused with the Children's Online Privacy Protection Act, COPPA). Compared to the broader CDA, COPA more narrowly focused on Internet content deemed harmful to minors. It too was subject to a lawsuit and was found unconstitutional by the federal Third Circuit Court of Appeals in June 2000. After a hearing before the Supreme Court, the case was remanded back to the Third Circuit which again found COPA unconstitutional a second time in March, 2003. The Supreme Court ruled that the law violates the constitutional protection of free speech. As of 2010, the law remains unconstitutional and unenforced.

2. E-rate Compliance and Certification

Q: Under what circumstances does my school or library have to comply with CIPA/NCIPA/BDIA?

A: To receive E-rate discounts your school or library has to comply with CIPA/NCIPA/BDIA as shown below.

Program	Must Comply with CIPA Requirements	CIPA Requirements Do Not Apply
E-rate	When getting discounts for • internal connections • Internet access	When getting discounts for • telecommunication services (voice or data)
ESEA Title IID and LSTA	When using funds for • purchasing computers that access the Internet • direct costs for accessing the Internet	When using funds for • any other purposes allowed by the program and state program guidelines

NCIPA is applicable only when getting E-rate discounts for internal connections or Internet access.

The Federal Communications Commission (FCC) is charged with enforcing CIPA/NCIPA/BDIA for the Erate program. The federal Department of Education (USDoE) and the federal Institute for Museum and Library Services (IMLS) are charged with ESEA and LSTA CIPA enforcement

respectively. A school or library getting E-rate discounts and ESEA or LSTA funding needs to comply with CIPA's E-rate requirements. The FCC released detailed CIPA/NCIPA regulations in April 2001. Those regulations are cited throughout this brief. The regulations give schools and libraries considerable latitude on how to implement the mandates in the law. Neither the USDoE nor the IMLS have developed detailed regulations. CIPA/NCIPA/BDIA are in no way governed by the North Carolina Department of Public Instruction or the State of North Carolina.

To determine whether an E-rate eligible service falls under the purview of the act, consult the SLD's Eligible Services List (ESL). In general, applicants with services that are defined in the Internet or internal connections part of the ESL must comply with the law. Applicants with services defined in the telecommunication services area of the list are exempt from compliance for telecommunication services only. If your telecommunications provider is also providing your school or library's Internet access, you must still comply with CIPA's filtering provision if you get E-rate Internet discounts from your provider. If a telecommunications provider bundles the cost of the circuit with its Internet service, and you want to get discounts on the circuit without needing to comply with CIPA, it will be necessary to have the circuit costs broken out (e.g., separate line item on the bill) to be able to get discounts only on the circuit.

Q: What is the impact of the Supreme Court's decision and the FCC's follow-up Order on library compliance with CIPA's filtering requirement?

A: On June 23, 2003, the Supreme Court ruled 6–3 that the filtering requirement in CIPA is constitutional for public libraries. This action reversed a 2002 federal district court ruling that had found the filtering mandate unconstitutional on First Amendment grounds. This decision means that any public library using E-rate funds for purposes outlined above will need to comply with CIPA's filtering requirement. Following the Court's ruling the FCC released its Order on library compliance with CIPA on July 24, 2003. Especially critical in the Order are paragraphs 11-13 which have information on the timeframe for 2003 certification and the filing of the newly revised E-rate forms. (See also the following question on 2003 certification.)

Highlights of the July 24, 2003 FCC Order.

- In part, because the FCC recognized the need of libraries to budget for costs associated with filtering technology and to plan for its implementation, the Commission gave libraries until the start of 2004

services to comply with CIPA's filtering mandate. For most libraries this was July 1, 2004.

- The Order is clear that during the current 2003 E-rate funding year libraries need to (A) be already compliant with CIPA's filtering provision, or (B) be undertaking actions to comply with the filtering provision by start of 2004 services.
- The Order also references the need for libraries to develop a policy and procedure to unblock sites when requested to by an adult patron. This reinforces the language in the Supreme Court's ruling that libraries that do not unblock sites when requested by adult patrons face an increased risk of legal challenges by patrons. (See the question on unblocking below.)
- It is important to note that the Order focuses on issues associated with the timeframe for compliance by libraries. Most of the FCC's original CIPA regulations, issued in April 2001, are still valid.

IMLS action: On August 1, 2003 the federal Institute of Museum and Library Services (IMLS) released its guidelines for complying with CIPA when using LSTA funds. Upon receiving FY 2004 LSTA funds public libraries were required to certify either that (A) the library was in compliance with CIPA's provisions, or (B) the library was undertaking actions to comply by the time it started using 2005 funds.

Schools were not part of the CIPA lawsuit. Most schools needed to comply with the law's filtering requirement as of July 1, 2002.

Q: How do we certify that we are meeting the law's requirements?

A: Certification of compliance is made by an appropriate "Administrative Authority" on the E-rate Form 486. This can be the school or library board, superintendent, principal, library director, or any other staff member with the authority to make such a certification. There are three certification options on the Form 486, item 11. In brief, these are:

A. My school or library has complied with the requirements of CIPA and NCIPA.

B. My school or library is "undertaking actions" to comply with requirements of CIPA and NCIPA.

C. CIPA and NCIPA do not apply because my school or library is receiving discounts only for telecommunications services.

Applicants must select the option that describes their state of compliance. For most applicants this will be either option A or C above. To prevent the loss of E-rate discounts, the Form 486 must be postmarked no later than:

- 120 calendar days after the Service Start Date listed on your Form 486 or
- 120 calendar days after the date of the Funding Commitment Decision Letter whichever is later. Most applicants with services starting July 1 of the funding year must file the 486 generally by October 28 of the same funding year. Monitor the SLD Website for the exact 486 deadline date.

Undertaking actions, option B:

The undertaking actions option is valid only the first time the school or library files for E-rate discounts after passage of CIPA/NCIPA. This is known as the "first funding year" and is triggered when a Form 486 is filed for Internet or internal connections and the 486 has been processed by the SLD.

For schools and libraries that are part of a consortium application, the Form 486 certification is submitted to the SLD by the Billed Entity. This is usually the consortium itself which filed the Form 471. Each member of the consortium (the "administrative authorities") must complete Form 479 declaring compliance with CIPA. The 479 forms are not submitted to the SLD but are collected and kept on file by the Billed Entity. For consortium applications that are only for telecommunication services, no 479 forms are required. Under such circumstances the Billed Entity simply checks the CIPA "does not apply" box on Form 486, #11c. If a consortium application includes some applicants that are getting Internet discounts and some that are getting telecommunication discounts, then all applicants that are part of the consortium must file Form 479 with the Billed Entity. See the Form 486 instructions for more information on consortium applications.

The FCC has ruled that if any member of a consortium application is not in compliance with the law, only the non-complaint members shall be subject to reimbursement of their proportional share of E-rate discounts. The other compliant members can continue to receive discounts (FCC regulations, ¶27).

Note: According to the FCC NPRM published in the Federal Register January 19, 2010, which includes proposed rule revisions related to BDIA, along with several other proposed rule revisions related to CIPA, the proposed rule revisions will not require any changes to the current Form 486 certifications. Likewise, according to the NPRM, the proposed rule revisions will not require

any changes to the Form 479, nor will consortium members need to file a revised Form 479. Consult the NPRM for more details.

Q. When will the FCC issue formal rules regarding the Protecting Children in the 21st Century Act?

A: As mentioned above the FCC NPRM published in the Federal Register January 19, 2010 contains proposed rule revisions related to BDIA. The FCC will vote on the proposed revisions following the comment and reply comment periods. The NPRM language is as follows.

1. The existing information collection requires schools and libraries to certify that they have in place certain Internet safety policies, pursuant to the Children's Internet Protection Act (CIPA), 47 U.S.C. 254(h) and (l), in order to receive E-rate discounts for Internet access.
2. This information collection is being revised to add a new certification that the E-rate applicant has updated its Internet safety policy to include plans for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response, as required by the Protecting Children in the 21st Century Act. This revision will not require any changes to the FCC Forms 479 or 486, which enable E-rate participants to certify that they are compliant with CIPA. This revision has no effect on the FCC Form 500, which is also part of this information collection. In addition, this information collection is being revised to add a rule provision requiring each Internet safety policy that is adopted pursuant to section 254(l) of the Act, as amended, to be made available to the Commission upon request by the Commission. Although this requirement is mandated by the statute, it is not currently in the Commission's rules.

Synopsis of the Notice of Proposed Rulemaking

1. In this notice of proposed rulemaking (NPRM), we propose revising the Federal Communications Commission's (Commission) rules regarding the schools and libraries universal service support mechanism, also known as the E-rate program, to comply with the requirements of the Protecting Children in the 21st Century Act. Among other things, section 215 of the Protecting Children in the 21st Century Act, titled Promoting Online Safety in Schools, revised section 254(h)(5)(B) of the Communications Act of 1934, as amended (the Act), by adding a new certification requirement for elementary and secondary schools that have computers with Internet access and receive discounts under

the E-rate program. We also propose to revise related Commission rules to reflect existing statutory language more accurately.

2. Under the E-rate program, eligible schools, libraries, and consortia that include eligible schools and libraries may apply for discounted eligible telecommunications, Internet access, and internal connections services. In accordance with the Children's Internet Protection Act (CIPA), to be eligible for E-rate discounts for Internet access and internal connection services, schools and libraries that have computers with Internet access must certify that they have in place certain Internet safety policies and technology protection measures. As required by CIPA, § 54.520(c)(i) of the Commission's rules requires that the Internet safety policy must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are (1) obscene, or (2) child pornography, or, with respect to use of the computers by minors, (3) harmful to minors. In addition, § 54.520(c)(i) requires the entity to certify that its policy of Internet safety includes monitoring the online activities of minors. Applicants make their CIPA certifications annually on the Confirmation of Receipt of Services Form (FCC Form 486).
3. Among other things, the Protecting Children in the 21st Century Act revised section 254(h)(5)(B) of the Act added a new certification for elementary and secondary schools that have computers with Internet access and receive discounts under the E-rate program. In addition to the existing CIPA certifications required of schools in section 254(h)(5) of the Act, the Protecting Children in the 21st Century Act requires the school, school board, local educational agency, or other authority with responsibility for administration of the school to certify that ''as part of its Internet safety policy [*it*] is educating minors about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms, and cyberbullying awareness and response.''

3. Requirements

Q. What are the basic requirements of CIPA?

A: A school or library must have some type of filter or blocking technology on all of its computers with Internet access. The filters must protect against access to certain visual depictions described in section III A below (CIPA requirement). In the future, the FCC may provide additional guidance.

Q. What are the basic requirements of NCIPA?

A: A school or library must have an Internet safety policy and hold a public meeting, before which reasonable public notice is provided, to review the policy. The policy must incorporate the criteria described in section III B below (NCIPA requirement). For schools, the policy must also address monitoring the online activities of minors. The law does not require "tracking of Internet usage by any identifiable minor or adult user."

Q. What are the basic requirements of BDIA?

A: A school's Internet safety policy must include educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

3. A. CIPA: Technology Protection Measure, TPM (Filtering)

Q: What does the law mean by "technology protection measure" (TPM)?

A: The term "technology protection measure" appears throughout the law. The best way to define this is to review the actual text of the act itself which says, "The term 'technology protection measure' means a specific technology that blocks or filters Internet access to visual depictions" defined in the act. In this brief Technology Protection Measure and filter are used interchangeably. A TPM may include other options, besides commercial Internet blocking and filtering software, including open source.

Q: What has to be filtered or subject to the TPM?

A: The law does not require the filtering of text. But the TPM must protect against access to visual depictions that are:

1. Obscene: This is defined in a reference to section 1460 of title 18, U.S. Code.
2. Child pornography: This is defined in a reference to section 2256 of title 18, U.S. Code.
3. Harmful to minors: This is applicable only to Internet access by minors. It is defined in CIPA and means any picture, image, graphic image file, or other visual depiction that:

a. taken as a whole, appeals to a prurient interest in nudity, sex, or excretion;

b. depicts, describes, or represents, in a patently offensive way, 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.

In its April 2001 rules, the FCC declined to elaborate on the banned visual depictions beyond what is already stated in the law (FCC regulations, ¶48). In addition to sexually explicit content, most commercial filtering programs have a variety of categories by which they can filter, including Web content related to games, gambling, drug use, violence, etc. Whether a school or library filters any content besides the visual depictions defined in the law is a local decision. However, libraries that filter other content open themselves to potential legal challenges based on the blocking of constitutionally protected content. The law, while defining the type of images that need to be blocked, does not specify any particular software (client) programs, such as a Web browser, email, or chat software which must come under the scrutiny of the TPM.

Q: What computers must have the Internet TPM?

A: The law states that a TPM that protects against access to the visual depictions referenced in the act must be on any of its computers with Internet access (CIPA section 1721 (a) (C)(i)). This includes student, staff, and patron computers accessed by minors or adults. The law makes no distinction between computers used only by staff and those accessible to the public. Therefore, even Internet connected computers located in administrative areas not accessible to the public or students must still have filters (FCC regulations, ¶30), but the TPM can be disabled. The FCC declined to make a specific filter exception for text-only terminals connected to the Internet. However, since such terminals cannot access the visual depictions outlawed by CIPA, this in itself probably constitutes compliance with the law (FCC regulations, ¶29). As described in the next question, a provision in the law allows the filter to be disabled under certain circumstances for adult Internet access.

Patron PCs: An increasingly popular option in libraries is to allow patron owned laptops to access the Internet through the library's wireline or wireless network. CIPA references the need for the library to have a TPM in place, "with respect to any of its computers with Internet access [emphasis

added]." It is very reasonable to assume that "its" refers to the library's PCs and that patron laptops need not be filtered. Officials at a federal agency have indicated, off the record, that they agree with this assumption.

The FCC has also stated that a school or library cannot prorate its E-rate discount to allow some computers to be unfiltered. For example, a library cannot say it will take only 50% of its authorized E-rate Internet discount and then leave 50% of its computers unfiltered.

Q: Under what circumstances or conditions can the TPM be disabled?

A: The law states that any authorized school or library staff may disable the TPM to allow adults to have unrestricted Internet access for any lawful purpose (CIPA section 1721 (6) (D)). Such staff authorization is granted by the school or library's governing body. The disabling language for E-rate is applicable to adults only (age 17 or older). Note: Even without CIPA, there is no constitutional protection for anyone to view obscene images, and child pornography, regardless of its medium, is clearly illegal.

The FCC in its April 2001 regulations stated that the method or procedures used to disable the TPM for adults is a matter of local school or library policy. The law provides no guidance in this area, and the FCC declined to provide any further clarification. Thus staff have considerable flexibility on how to implement the disabling provision. The Supreme Court's ruling notes "the ease with which patrons may have the filtering software disabled." However, frequent requests for disabling can be time consuming for staff to administer, and may be technologically difficult and costly to implement. The FCC regulations say that if there are concerns about "costs associated with maintaining filtering or blocking systems that may frequently be disabled" then libraries should take the cost considerations into account when evaluating any technology protection measures (FCC regulations, ¶30).

The Supreme Court's plurality opinion and the concurring opinions of Justices Kennedy and Breyer place considerable emphasis on CIPA's unblocking option. The optional "may disable" language in the law has on taken on a "must disable" interpretation by the Court's ruling. For example, Justice Kennedy's concurring opinion indicates that if a patron requests unfiltered access to view constitutionally protected Internet material, and the library (1) refuses such a request, (2) does not have the technical ability to grant such a request, or (3) places some other undue burden on the patron, then the library places itself at risk of an "as-applied" challenge by the patron. "As-applied" meaning that as the library has applied CIPA's filtering mandate, the patron contends it is unconstitutionally blocking access to legal content. (See also the question, "What are the legal

implications…?")

The law does not address the issue of requiring patrons to state why they are seeking unfiltered Internet access or the type of information they are seeking. (Of interest, there is no language in CIPA that states patrons need to ask staff to disable the filter.) During the Supreme Court's oral argument, the Solicitor General stated that a patron does "not have to explain any reason why he was asking a site to be unblocked or the filtering to be disabled." This phrasing is quoted in the Court's plurality decision. Thus there is considerable legal support that says patrons simply have to request unfiltered access to legal content on the Internet, with no explanation needed. Considering this, a library policy of having staff ask patrons why they want unfiltered access is very questionable from the Court's perspective and, in addition, such questions raise obvious issues of privacy and confidentiality. A library's AUP should address the issue of what constitutes a patron's acceptable or unacceptable use of the Internet without the need for intrusive staff interference.

Although the ESEA and LSTA sections of CIPA permit the disabling of filters for both adults and minors, no such disabling provision for minors is included in the E-rate section (SEC. 1721). No provision, however, prevents schools or libraries from setting different levels of filtering for minors on an age determinant or individual use basis.

In addition to the three types of material that schools or libraries must attempt to block, CIPA explicitly permits schools and libraries to block any content deemed inappropriate for minors by local standards.

Staff workstations: Unlike a patron request for unfiltered access, which is based on the First Amendment, a staff request for unfiltered access is more of a management or board decision.

The procedure for disabling the TPM is a decision to be made by each school or library in close consultation with the board and legal counsel as needed. And considering the importance that the Court has placed on disabling, this should be a key factor in any filter evaluation.

Note: School boards would be well advised to address Internet use and TPM disabling procedures for "patrons" in its Internet policy given the fact that the FCC is preparing to vote on "An Order and Notice of Proposed Rulemaking to enable schools that receive funding from the E-Rate program to allow members of the general public to use the schools' Internet access during non-operating hours at no additional cost to the Universal Service

Fund. This order and notice do not permit or require any changes to E-Rate applications due on February 11, 2010."

Q: How effective does the TPM have to be? Is there any type of TPM effectiveness certification?

A: It is important to note that the law states that the TPM must protect against visual depictions outlawed by the legislation. The TPM does not have to prevent access to all such depictions. (No TPM is 100% effective in preventing all such access.) In developing its CIPA regulations, the FCC declined to further define the filter requirements or to adopt any type of definition or certification on how effective a filter must be, beyond the very general "protect" language of the law. Thus, there is no such thing as an FCC certified TPM or a CIPA certified TPM. And, considering the broad interpretation of the word "protect," any statements by vendors that their filtering software will help schools and libraries be CIPA compliant are of limited value.

The FCC regulations do not require schools or libraries to track the number of attempts made to access prohibited visual depictions or the number of times the TPM succeeds or fails. The regulations also do not require schools or libraries to collect any complaints filed by staff, students, or the public on what was or was not blocked (FCC regulations, ¶42). The school or library's Internet policy may indicate that it will track and collect such statistics, but there is no mandate to do this in the law or regulations. (During the open public comment period before release of its regulations in April 2001, some organizations requested the FCC to mandate such tracking and compiling of complaints.)

Q: What are the legal implications if the TPM fails and allows banned images to appear on the screen?

A: The FCC presumes that Congress did not intend to penalize schools or libraries that act in good faith and in a reasonable manner to implement filters. The FCC also notes that failure to comply with the law's requirements "could also engender concern among library patrons and parents of students at the school. We believe that schools and libraries will act appropriately in order to avoid such outcomes." (FCC regulations, ¶47) In other words, the FCC will rely, in part, on community "concern" to serve as one mechanism to enforce compliance.

There may still be instances in which a patron, parent, student or staff member claims that too many allegedly obscene images are getting through the TPM. A school or library must have policies and procedures in place if it

is to address any such complaints expeditiously. It is possible that a complaint with the FCC could be initiated that would prompt an investigation. Under CIPA, the FCC can require a school or library to reimburse its E-rate discounts for any period of time it was out of compliance. However, the FCC has stated that it is not in a position to make a legal determination that an image is obscene. This can only be done as part of a formal court procedure following legal standards, such as those established by the Supreme Court in Miller v. California. To reemphasize: Having a policy to address complaints can help minimize any possibility of more formal legal action.

Q: Does it make any difference where the filtering takes place?

A: It makes no difference where the filtering is done. It can be done centrally by an Internet Service Provider (ISP) or at the server level on the school or library's LAN or WAN, or the filter can be individually installed on each computer, or any combination of the above.

Q: How will the May 20, 2010 FCC NPRM impact CIPA compliance?

A: On May 20, 2010, the FCC released a Notice of Proposed Rule Making (NPRM) FCC 10-83 to propose revising the E-rate program to support the goals of the National Broadband Plan and to cut red tape. In this seminal NPRM the FCC requests comments on a number of significant changes to the E-rate program. Two potential changes could impact CIPA compliance. 1. The FCC proposes: "to adopt the National Broadband Plan recommendation to provide full E-rate support for wireless Internet access service used with ~~a~~ portable learning devices that are used off premises." Current rules require any "at home" use to be cost allocated. Conceivably, the current CIPA rules would apply to the eligible service regardless of location; hence the requirement to filter any of "its" computers with Internet access would thus apply. In addition, the NPRM seeks comment regarding the need for additional local policy requirements related to this potential rule change. 2. The FCC seeks comment: "on whether we should allow schools that serve unique populations to receive E-rate funding for priority one and priority two services delivered to residential areas. Conceivably, the current CIPA rules would apply to the eligible service regardless of location; hence the requirement to filter any of "its" computers with Internet access would thus apply.

3. B. Internet Safety Policy and Public Meeting (NCIPA)

NCIPA's requirements apply only when getting E-rate discounts for services referenced under CIPA. NCIPA does not apply when using just LSTA or ESEA funds for purposes referenced in CIPA.

Note: Assuming the school or library is not in its first E-rate year in reference to NCIPA (see *undertaking actions* paragraph above), the school or library should already have an Internet Safety Policy and should have already held a public meeting on the policy.

Q: What should have been included in our policy prior to BDIA?

A: The CIPA section of the law says that a school or library must have an Internet safety policy and this policy must include the use of filters to protect against access to the visual depictions outlawed in the act. The school's Internet policy must also indicate how it plans to monitor the Internet activities of minors. The law does not require this monitoring provision in the public library's policy. Note: Neither the law nor the FCC rules require the actual online tracking of Internet use by minors or adults.

The NCIPA section of the law is much more specific in its safety policy requirements. NCIPA requires that schools and libraries participating in the E-Rate program adopt and implement an Internet safety policy that addresses:

1. Access by minors to inappropriate matter on the Internet and the Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

Q: One of the requirements refers to access by minors to "inappropriate matter" and another refers to access to "materials harmful" to minors. What's the difference?

A: The term "materials harmful to minors" is defined in CIPA as cited above. The definition of "inappropriate matter" is to be made by the school or library board or administration. The law states that the federal government

is not to make any determination on what is or is not "inappropriate for minors." CIPA defines a minor as any person less than 17 years of age.

Q: Does the Internet Safety Policy have to be adopted by the school or library board, or can it be done as an administrative procedure?

A: The law says the "school or library" shall adopt and implement a policy that meets the requirements of the law. Though the law does not state specifically that the board must pass the policy, it is prudent to have your board take such action.

Q: Can a regular meeting of the school or library board be used as the required public meeting?

A: The law and the regulations give schools and libraries considerable flexibility in meeting the public hearing mandate. The law says simply that schools or libraries must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." Considering this general language, the hearing can be part of a regular board meeting, assuming such a meeting allows for public comments. Notices of such a meeting must comport with any local or state open meeting laws. Be certain to document fully the public meeting by keeping a copy of the notice, noting any actions taken, etc.

3. C. Internet Safety Policy and Online Safety Education (BDIA)

Q: Can we use our acceptable use policy or current Internet safety policy as the CIPA/NCIPA/BDIA Internet safety policy?

A: You can use your current Internet policy only if it meets all the requirements stated in the legislation, as amended in 2008. If, after reviewing your policy, you determine that it does not meet the current law's requirements, then you will have to initiate a process to revise it so that it is in compliance. As an example, an acceptable use policy that focuses on student and staff behavior, may not fully address staff monitoring and education responsibilities.

Q. Does the Internet policy have to be named "Internet safety policy?"

A: This is not an FCC rule, nor is it a requirement of the law, however, to indicate CIPA/NCIPA/BDIA compliance to stakeholders and potentially to auditors, it would be useful to include the words "Internet safety policy" in the title or introductory text.

Q. Who evaluates a school or libraries Internet safety policy?

A: The FCC has not established any specific criteria for evaluating an Internet safety policy, nor has NCDPI.

Q. How are schools to incorporate Internet safety instruction?

A: The FCC has not established any specific criteria for incorporating Internet safety instructions, nor has NCDPI. The North Carolina Attorney General's office offers Internet safety presentations as does NCDPI and many others. Districts are free to develop their own curriculum, use free Internet safety resources, or purchase commercial Internet safety packages.

Q. Who will evaluate the effectiveness of the online safety education.

A: While the FCC has not established any specific criteria for evaluating the effectiveness of an online safety education or digital citizenship program, independent auditors, contracted by the FCC, OIG, et al. will no doubt develop checklists that specifically include "social networking, chat rooms, and cyber bullying awareness and response.

4. Sources for More Information

FCC Consumer Facts on Children's Internet Protection Act (CIPA)
(http://www.fcc.gov/cgb/consumerfacts/cipa.html)
• What CIPA requires fact sheet published by the FCC.

Información para el Consumidor - Ley de Protección de Niños en Internet (CIPA) (http://www.fcc.gov/cgb/consumerfacts/spanish/cipa.html)
• Información para el Consumidor publicados por la FCC.

FCC Protecting Children in the 21st Century Act Public Notice, (2010)
(http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-102A1.pdf)
• FCC comment request on the E-rate program and compliance with the Protecting Children in the 21st Century Act.

FCC National Broadband Plan E-rate NPRM (2010)
(http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-83A1.pdf)
• FCC comment request on proposed significant changes to the E-rate program to support the goals of the National Broadband Plan and to cut red tape.

FCC April 2001 CIPA Regulations
(http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc)
• These are the FCC's regulations released April, 2001. The regulations outline the specific actions schools and libraries must take to comply with CIPA and NCIPA.

FCC July 2003 CIPA Regulations for Libraries
(http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-188A1.doc)
• These are the FCC's regulations specifically related to the timeframe for library compliance with the Supreme Court's ruling on CIPA's filtering mandate.

SLD CIPA and Form 486 Frequently Asked Questions
(http://www.sl.universalservice.org/reference/CIPAfaq.asp)
• A good, detailed FAQ on the key relationship of CIPA to the E-rate's Form 486.

FAQ on CIPA and NCIPA (http://dpi.wi.gov/pld/cipafaq.html)
• FAQ on E-rate and the Children's Internet Protection Act, CIPA.

Supreme Court Decision
(http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf)
• The text of the Court's June 23, 2003 decision.

CIPA Challenge Documents (http://archive.aclu.org/features/f032001a.html)
• Extensive repository from the ACLU with links to many documents related to the legal challenge to CIPA.

ALA CIPA Site (http://www.ala.org/cipa)
• Good site with the latest legal and regulatory information, etc. See also the memo on filter disabling options including the outline of several possible scenarios that involve minimal staff involvement at:
http://www.ala.org/ala/washoff/WOissues/civilliberties/washcipa/qanda/q.htm

Coping with CIPA: A Censorware Special
(http://cites.boisestate.edu/civ3i9.pdf)
• A special CIPA issue of Walt Crawford's Cites and Insights. A very good review with many quotes from newspaper editorials and perspectives, both supporting and opposing the Court's decision.

CIPA Update
(http://www.infopeople.org/training/webcasts/handouts/2003/7-17-03_handout_files/CIPAsent.pdf)
• This is the handout used as part of a July 2003 CIPA update from Mary

Minow. It provides a good overview of the law and the Court's decision.

Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries (http://eratecentral.com/CIPA/cipa_policy_primer.pdf)
• In addition to a review of the act, this paper contains Internet Safety Policy guidelines and a sample compliant Internet Safety Policy. From E-rate Central.

Analysis of the CIPA Decision
• FindLaw columnist, attorney, and author Julie Hilden argues the recent CIPA Court decision is less destructive to free speech rights than it seems.

ALA Libraries & the Internet Toolkit
(http://www.ala.org/ala/oif/iftoolkits/litoolkit/librariesinternet.htm)
• A good variety of background papers, policies, FAQs, etc., to help librarians manage and communicate about the Internet.

Plain Facts About Internet Filtering Software.
(http://www.ala.org/ala/pla/plapubs/technotes/internetfiltering.htm)
• Provides a good overview of how filters work, a filter check list and a good bibliography. (This is a PLA Tech Note authored by Karen G. Schneider.)

Loudoun County (VA) Library Internet Filters Case Summary
(http://www.eff.org/Legal/Cases/Loudoun_library/)
• This was the first legal challenge to filters in libraries to reach the federal courts.

Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries

Prepared by E-Rate Central

The Children's Internet Protection Act ("CIPA"), enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act ("NCIPA") that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act, enacted October 10, 2008, adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

Introduction to CIPA Compliance

CIPA (and the associated NCIPA) requirements for E-rate purposes are governed by rules promulgated by the Federal Communications Commission ("FCC") and administrated by the Schools and Libraries Division ("SLD"). The basic FCC rules are summarized below.

1. Applicability: CIPA compliance is required for any school or library receiving E-rate funds for three of the four eligible service categories – Internet Access, Internal Connections, and Basic Maintenance. Applicants for Telecommunications services only, are exempt.

2. Timing: Full compliance is required in an applicant's second year of funding after CIA's enactment. For most applicants, this was the fifth E-rate program year ("PY5" or "FY 2002") beginning July 1, 2002. For the preceding year, an applicant needed only to certify that it was "undertaking actions" to be in compliance for the second year.

3. Filtering: CIPA requires the implementation of a "technology protection measure" – generally referred to as an Internet filter – to block access to visual depictions deemed "obscene," "child pornography," or "harmful to minors."[1] Filtering is required for all of an E-rate recipient's Internet-enabled computers whether used by minors or adults. For E-rate funding purposes, filtering for adult Internet usage can be disabled for "bona fide research or other lawful purpose."[2]

---

[1] The terms "obscene," "child pornography," and "harmful to minors" are strictly and legally defined (see footnote to the sample Internet Safety Policy in Appendix B).

[2] Although the ESEA and LSTA sections of CIPA permit the disabling of filters for both adults and minors, no such disabling provision for minors is included in the E-rate section (SEC. 1721). No provision,

The FCC has not established any standards with regard to the type or effectiveness of Internet filters required for CIPA compliance.

4. Internet Safety Policy: CIPA requires the adoption and enforcement of an "Internet safety policy" covering the filtering discussed above.[3] For schools, the policy must also address "monitoring the online activities of minors."[4]

   NCIPA provisions, applicable to E-rate recipients, requires the policy to address the following five components:

   - 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 (including instant messaging);
   - Unauthorized access, including so-called 'hacking,' and other unlawful activities by minors online;
   - Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
   - Measures designed to restrict minors' access to materials harmful to minors.[5]

   A separate, but related, provision of the Protecting Children in the 21st Century Act requires that the policy include measures for educating minors about appropriate online behavior.

   Prior to adoption, CIPA requires that "reasonable public notice" and "at least one public hearing or meeting" be held to address the proposed Internet safety policy.

   The FCC has not established any specific criteria for evaluating an Internet safety policy, nor has it set any specific standards for what constitutes reasonable public notice or a public meeting.

5. Certification: The only specific compliance requirement established by the FCC is that an E-rate applicant must certify that it is in compliance with the CIPA provisions summarized above. Certification is required only after funding is awarded by filing a Form 486 indicating receipt of services.[6] Certification is required annually.

---

however, prevents schools and libraries from setting different levels of filtering for minors on an age-determinant or individual use basis.

[3] In addition to the three types of material that must be blocked, CIPA explicitly permits schools and libraries to block any content deemed inappropriate for minors by local standards.

[4] "Monitoring" appears to require only supervision, not technical measures. Specifically, CIPA does not require "tracking of Internet usage by any identifiable minor or adult user."

[5] Not just visual depictions.

[6] Members of a consortium must certify status on Form 479s that must be submitted to the consortium leaders before the leader files a consortium-wide Form 486.

6. Enforcement: No specific enforcement provisions, other than applicant certifications on FCC Form 486, have been established by the FCC. The only two principles of enforcement are:

   - No Universal Service Fund payments will be made on behalf of any applicant that does not file the requisite certifications; and
   - If certifications are found to be false — as determined by subsequent review or audit — applicants will have to reimburse the Fund for any funds and discounts received for the period covered.

Internet Safety Policy Guidelines

Although neither the FCC nor the SLD has established specific criteria for an Internet safety policy, certain practical guidelines can be suggested as a means of complying with the CIPA policy requirements.

Basic Components of a CIPA-compliant Internet Safety Policy:

At a minimum, to fully comply with the spirit of the Internet safety policy requirements for E-rate funding, four key guidelines should be met.

1. The policy should apply to both minors and adults. Although called the "Children's Internet Protection Act," and requiring specific protections for minors, CIPA clearly applies to certain aspects of adult usage as well. Therefore, the policy should deal with both staff and students (or library patrons). As discussed below, a student Acceptable Use Policy may not fully suffice.

2. The policy should specify use of an Internet filtering mechanism to, at a minimum, block access to the three categories of visual depictions specified by CIPA – obscene, child pornography, and harmful to minors. Conditions and procedures should be incorporated under which filtering can be disabled (for adults) or made less restrictive (for minors).

3. The policy should emphasize staff responsibilities in educating minors on appropriate online behavior and in supervising such activities. This provision is needed to meet the monitoring and education requirements imposed on schools and libraries.

4. The policy should address the NCIPA issues for minors (but is also appropriate for adults). As discussed above, these issues concern the safe use of e-mail and other forms of electronic messaging, unauthorized disclosure of personal information, and unlawful online activities.

A sample Internet safety policy, minimally addressing these four CIPA-related guidelines, is provided in Appendix B.

Optional Internet and Network Policy components:

The sample Internet safety policy provided in Appendix B is designed solely to meet the basic E-rate requirements for CIPA compliance. Although not the primary purpose of this Primer, it should be noted that many schools and libraries may already have, or may wish to adopt, much broader policies addressing other Internet or network issues. A brief summary of other typical policy components is provided below. Several examples of broader policies are provided in the Internet links listed in Appendix A.

1. Statement of objective. Discussion as to the purpose and importance of the organization's computer network and Internet access. Access to these resources may be designated a privilege, not a right.

2. Penalties for improper use. Failure to adhere to network policies and rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings.

3. Organizational responsibility and privacy. Disclaimers indicating that:
   - The organization does not warrant network functionality or accuracy of information.
   - The organization does not warrant the effectiveness of Internet filtering.
   - The privacy of system users is limited.

4. Acceptable use. Provisions dealing with such issues as:
   - Network etiquette.
   - Vandalism and harassment (e.g., "cyberbulling").
   - Copyrights and plagiarism.
   - Access to social networking or chat room Web sites.
   - Downloading (e.g., music files)

5. Web site. Special provisions dealing with the use and modifications of an organization's own Web site.

6. Personnel responsibilities. Designation of an organization's personnel who are responsible for various aspects of network and user administration and use.

Review and Revision of Existing Policies:

Many schools and libraries may have existing policies in place that fully, or at least partially,[7] meet the CIPA requirements for an Internet safety policy. If a review indicates the need for a revision, the following suggestions are offered for consideration:

[7] An acceptable use policy for students, for example, may cover many aspects of student behavior, but may not address adult staff usage, monitoring, and education responsibilities.

1. Title. To indicate CIPA compliance, it would be useful to include the words "Internet safety policy" in the title or introductory text.

2. Specific terms. Terminology may be important to CIPA compliance.
   a. Prohibited activity should specifically include access to material deemed "obscene," "child pornography," or "harmful to minors."
   b. Reference should be made to supervision or "monitoring" of online activities by minors.
   c. References to disabling of filtering should refer to "disabling or relaxing" for "bona fide research or other lawful purposes."

3. Specific problems. Although not a CIPA issue, it may be appropriate to expand portions of earlier policies to deal more explicitly with problems recently faced by schools and libraries such as student and staff harassment, plagiarism, and copyright violations.

4. Adult usage. The policy should address usage by adults, not simply students and/or minors. Adult-oriented policies are becoming commonplace in corporate and governmental organizations to establish standards of behavior for network usage.

5. Companion policies. Schools, with an existing student-oriented acceptable use policy, may be able to adopt a broader, but simpler, Internet safety policy referencing the acceptable use policy.

6. Public hearing. Revised, CIPA-compliant, Internet safety policies should be adopted in a pre-announced public meeting. A regular school or library board meeting, at which the policy adoption is listed in a pre-released agenda, should be sufficient.

Appendices:

Appendix A – Internet links for further information

Appendix B – Sample, CIPA-compliant, Internet safety policy

Internet Links for Additional Information on CIPA and Internet Safety Policies

CIPA Background

- Full text of the Children's Internet Protection Act
  http://www.ifea.net/cipa.html
- FCC regulations implementing CIPA; FCC 01-120
  http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-01-120A1.pdf
- SLD's FAQ on E-rate certification procedures and timing
  http://www.sl.universalservice.org/reference/CIPAfaq.asp

Internet Safety Policies and Issues

- Resources from the American Library Association ("ALA")
  http://www.ala.org/ala/aboutala/offices/wo/woissues/civilliberties/cipaweb/cipa.cfm
- NTIA Study of Technology Protection Measures
  http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/CIPAreport_08142003.htm
- Full text of the related Children's Online Privacy Protection Act ("COPPA") governing the operation of Web sites re. unfair and deceptive acts in connection with the collection and use of personal information from and about children
  http://www.ftc.gov/ogc/coppa1.htm
- Full text of the Protecting Children in the 21st Century Act is included as Title II of the Broadband data Information Act, S.1492 (in particular, see Sec.215)
  http://www.govtrack.us/congress/billtext.xpd?bill=s110-1492

Sample CIPA-Compliant Internet Safety Policy

Note: The following Internet safety policy was developed by E-Rate Central solely to address the basic policy compliance requirements of CIPA and NCIPA for E-rate funding. Schools and libraries adopting new or revised Internet policies may wish to expand or modify the sample policy language (as suggested in the accompanying Primer) to meet broader policy objectives and local needs. Neither the FCC nor the SLD has established specific standards for a CIPA-compliant Internet safety policy and neither has reviewed, much less endorsed, this sample policy.

Internet Safety Policy For <School or Library>

Introduction

It is the policy of <School or Library> to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.*

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the <School or Library> online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the <School or Library> staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of <Title> or designated representatives.

Adoption

This Internet Safety Policy was adopted by the Board of <School or Library> at a public meeting, following normal public notice, on <Month, Day, Year>.

---

* CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term ``harmful to minors'' means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. 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
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms ``sexual act'' and ``sexual contact'' have the meanings given such terms in section 2246 of title 18, United States Code.