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.

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 administered by the Schools and Libraries Division ("SLD"). The basic FCC rules are summarized below.

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

2. <u>Timing</u>: Full compliance is required in an applicant's second year of funding after CIA's enactment. For most applicants, this will be the fifth E-rate program year ("PY5") beginning July 1, 2002. For the preceding year (PY4 for most), an applicant need only certify that it is "undertaking actions" to be in compliance for the second year.

3. <u>Filtering</u>: CIPA requires the implementation of a "technology protection measure" – generally referred to as an Internet filter – to block access to <u>visual</u> 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 provision for minors is included in the E-rate section (SEC. 1721). No provision, however,

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

4. <u>Internet Safety Policy</u>: 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, also require a policy to address:

   - "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]

   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. <u>Certification</u>: 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.

6. <u>Enforcement</u>: No specific enforcement provisions, other than applicant certifications, have been established by the FCC. The only two principles of enforcement are:

---

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 <u>identifiable</u> 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.

- 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 supervising online activities by minors. This provision is needed to meet the "monitoring" requirement imposed on schools (but also appropriate for 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. <u>Statement of objective</u>. 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. <u>Penalties for improper use</u>. Failure to adhere to network policies and rules may subject users to warnings, usage restrictions, disciplinary actions, or legal proceedings.

3. <u>Organizational responsibility and privacy</u>. 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. <u>Acceptable use</u>. Provisions dealing with such issues as:

   - Network etiquette.

   - Vandalism and harassment.

   - Copyrights and plagiarism.

   - Downloading (e.g., music files)

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

6. <u>Personnel responsibilities</u>. 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, 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:

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

2. <u>Specific terms</u>. 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. <u>Specific problems</u>. 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. <u>Adult usage</u>. 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. <u>Companion policies</u>. 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. <u>Public hearing</u>. 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.fcc.gov/ccb/universal_service/chipact.doc

- FCC regulations implementing CIPA; FCC 01-120
  http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc

- SLD's FAQ on E-rate certification procedures and timing
  http://www.sl.universalservice.org/reference/CIPAfaq.asp

Internet Safety Policies and Issues

- Sample administrative policies[7]
  http://www.open.k12.or.us/jitt/district/policy.html

- A legal and educational analysis of K-12 Internet policies[8]
  http://ces.uoregon.edu/responsibleuse/analysis.htm

---

[7] Documents co-developed under contract with Ms. Nancy Willard and licensed to all Oregon public school districts.

[8] © 1997 Nancy Willard.

Sample CIPA-Compliant
Internet Safety Policy

<u>Note</u>: 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.

Supervision and Monitoring

It shall be the responsibility of all members of the <School or Library> staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection 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.