On-Tech Consulting, Inc.
53 Elm Place
Red Bank, NJ 07701
Voice: (732) 530-5435
Fax: (732) 530-0606
www.on-tech.com
info@on-tech.com

E-Rate Funding—Guaranteed

CIPA, Libraries and the E-Rate

Dan Riordan

On-Tech Consulting, Inc.

dan@on-tech.com

Introduction

On-Tech is a technology consulting firm focused on managing the E-Rate process for schools and libraries. We provide a full range of E-Rate services for applicants, including: handling the entire application process; consulting on construction projects to ensure maximum E-Rate funding; and reviewing proposals to ensure E-Rate compliance. In addition, On-Tech obtains E-Rate funding for school and library construction projects. On-Tech is not associated with any service provider.

Dan Riordan has been involved with the E-Rate since 1997, when he was trained by the New Jersey Department of Education to offer assistance to school districts in completing the application. Since then, he has worked on the E-Rate as a trainer, a district technology coordinator, and now a consultant.

The History of CIPA

CIPA started in the year 2000, and has continued to evolve since then, with new regulations, court decisions and amendments to the law.

The Laws

The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA) passed Congress in December of 2000. 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.

The CIPA and NCIPA laws are available at:

http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/cipa/cipatext.pdf

Supreme Court Decision

On June 23, 2003, the Supreme Court ruled that the filtering requirement in CIPA is constitutional for public libraries. This decision means that any public library using E-Rate funds for purposes outlined above will need to comply with CIPA's filtering requirement. In addition, the Supreme Court required that libraries turn off filtering at patron request.

http://www.law.cornell.edu/supct/html/02-361.ZO.html

FCC Regulations

The Federal Communications Commission released its regulations for CIPA and NCIPA covering the E-Rate program in April 2001. The most recent amendment, which does not affect libraries, is effective July 2012. The regulations are in Appendix A.

CIPA Compliance Requirements

CIPA not required for all E-Rate funding

Applicants which are receiving funding only in the category of Telecommunications Services do not need to comply with CIPA. Only applicants applying for funding in the categories of Internet Access, Internal Connections and/or Basic Maintenance of Internal Connections need to comply with CIPA.

General compliance requirements

Internet Safety Policy

The library's policy must address:

1. access by minors to inappropriate matter on the Internet
2. 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 information regarding minors
5. measures restricting minors' access to materials harmful to them

Be careful in your policy to avoid terms like: Pornography, Sexually Explicit, Offensive, Inappropriate, and Indecent. It is better to stick to the terminology in the law: "obscene," "child pornography" and "harmful to minors."

Public Meeting

The Internet safety policy must be discussed at a public meeting: regular public meetings of a library board satisfy this requirement.

Technology Protection Measure

Applicants must have technology in place which blocks or filters Internet access to:

1. Obscene pictures: defined elsewhere in U.S. law; briefly, very hard core pornography only; prurient, patently offensive, lack any serious value; appeals to shameful, morbid interest in sex;
2. Child pornography pictures: defined elsewhere in U.S. law
3. Pictures harmful to minors (people under 17 years of age)
    a. "appeals to a prurient interest in nudity, sex or excretion"
    b. "depicts…[a] sexual act or sexual contact…or a lewd exhibition of genitals"
    c. "lacks serious literary, artistic, political or scientific value as to minors"
    d. Violence is not "harmful to minors"

The technology protection measure may be disabled during use by an adult.

For Schools Only

Schools have additional requirements. Schools must monitor online activities of minors, and must provide training for students in responsible use of the Internet.

Library compliance requirements

As a result of the Supreme Court decision, libraries are required to disable filtering when requested by patrons. The ALA has considered a number of ways to do this, and discussed their legality at:

http://www.ala.org/advocacy/advleg/federallegislation/cipa/cipascenarios

Colorado compliance requirements

Public libraries must take "reasonable measures must be adopted and implemented to protect the children who use such internet services in public libraries from access to material that is harmful to their beneficial development as responsible adults and citizens." The particulars of the bill mirror CIPA fairly closely.

http://www.cde.state.co.us/cdelib/LibraryLaw/Part6.htm

Deadlines for compliance

In general, applicants must be compliant before service starts. A library cannot request for any Internet Access, Internal Connections or Basic Maintenance services which were delivered while the library was not CIPA-compliant. Applicants certify CIPA compliance on the Form 486.

"Undertaking Actions"

Your library can receive funding if you are "undertaking actions" to comply with CIPA. An undertaken action is an action that can be documented and that moves the school or library toward compliance. Following are a few examples of documentation that could demonstrate that a school or library is "undertaking actions" to comply with CIPA:

- A published or circulated school or library board agenda with CIPA compliance cited as a topic
- A circulated staff meeting agenda with CIPA compliance cited as a topic
- A service provider quote requested and received by a recipient of service or Billed Entity which contains information on a technology protection measure
- A draft Request for Proposals or other procurement procedure to solicit bids for the purchase or provision of a technology protection measure
- An agenda or minutes from a meeting open to the public at which an Internet safety policy was discussed
- An agenda or minutes from a public or non-public meeting of a school or library board at which procurement issues relating to the acquisition of a technology protection measure were discussed
- A memo to an administrative authority of a school or library from a staff member outlining the CIPA issues not addressed by an Acceptable Use Policy currently in place
- A memo or report to an administrative authority of a school or library from a staff member describing research on available technology protection measures
- A memo or report to an administrative authority of a school or library from a staff member that discusses and analyzes Internet safety policies in effect at other schools and libraries

This list is not meant to be exhaustive.

Remember that such actions must occur before the start of services in order for discounts to be paid back to the Service Start Date reported on the Form 486.

Documenting compliance

Libraries should retain the following documentation for at least five years:

1. Internet Safety Policy
2. Minutes of public meeting where the Internet Safety Policy was discussed.
3. Proof of filtering
4. If necessary, proof the library was "undertaking action" to become compliant

Filters

What computers must be filtered?

All library-owned computers, including administrative computers, are covered by the CIPA requirements

If the library grants Internet access to patron laptops, those are not library-owned, and do not have to be filtered.

When can filters be disabled?

Filters can be disabled at an adult patron request. Some libraries have included such a request in the library Internet use agreement, so that all adult computers can be unfiltered.

When must filters be disabled?

Upon request, patrons must be given access to content harmful to minors. Patrons do not have a constitutional right to view information that meets the legal definition of obscene or child pornography.

How effective does the filter have to be?

No filter is 100% effective. Libraries must make a good faith effort to meet the filtering requirement.

What are some tools for filtering?

Information on some of the most popular tools is available at libraryfiltering.org.

OpenDNS is free, and is open source. Blocked lists are created by crowdsourcing.

Best practices

- The filter should implement standards set in Internet Safety Policy.
- Block as few categories as possible.
- When a site is blocked, it should tell patrons which URL was blocked and why.

More Resources

On-Tech

www.on-tech.com/erate

This handout and other E-Rate information and links are available at our Web site.

blog.on-tech.com

For a more informal discussion of the E-Rate, visit our blog. You can search for a topic of interest to you and get an insider's view.

If you have specific questions, contact us.

Email: info@on-tech.com
Phone: 732-530-5435

ALA

The American Library Association has many resources on CIPA:

http://www.ala.org/advocacy/advleg/federallegislation/cipa

The ALA also has a page on filtering, which overlaps with the CIPA page somewhat:

http://www.ala.org/advocacy/intfreedom/filtering

Finally, the ALA also has a page which gives legal guidance on satisfying CIPA requirements with currently available technology by looking at two possible scenarios:

http://www.ala.org/advocacy/advleg/federallegislation/cipa/cipascenarios

Schools & Libraries Division (SLD)

http://www.usac.org/sl/applicants/step10/cipa.aspx

LibraryFiltering.org

Information on filtering in general, and a comparison of many of the products available.

http://libraryfiltering.org/

Colorado Department of Education

The CDE has a very informative document describing Colorado's Library Internet Filtering Bill.

http://www.cde.state.co.us/cdelib/download/pdf/Interpretations.pdf

Appendix A: FCC Regulations

(6) Requirements for certain libraries with computers having Internet access

(A) Internet safety

(i) In general Except as provided in clause (ii), a library having one or more computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the library—

(I) submits to the Commission the certifications described in subparagraphs (B) and (C); and

(II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the library under subsection (l) of this section; and

(III) ensures the use of such computers in accordance with the certifications.

(ii) Applicability The prohibition in clause (i) shall not apply with respect to a library that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

(iii) Public notice; hearing A library described in clause (i) shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy.

(B) Certification with respect to minors

A certification under this subparagraph is a certification that the library—

(i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—

(I) obscene;

(II) child pornography; or

(III) harmful to minors; and

(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors.

(C) Certification with respect to adults

A certification under this paragraph is a certification that the library—

(i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—

(I) obscene; or

(II) child pornography; and

(ii) is enforcing the operation of such technology protection measure during any use of such computers.

(D) Disabling during adult use

An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

(E) Timing of implementation

(i) In general Subject to clause (ii) in the case of any library covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certification under subparagraphs (B) and (C) shall be made—

(I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and

(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

(ii) Process

(I) Libraries with Internet safety policy and technology protection measures in place A library covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application cycle under this subsection, except that with respect to the first program funding year after the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not later than 120 days after the beginning of such first program funding year.

(II) Libraries without Internet safety policy and technology protection measures in place A library covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)—

(aa) for the first program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and

(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any library that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such library comes into compliance with this paragraph.

(III) Waivers: Any library subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A library, library board, or other authority with responsibility for administration of the library shall notify the Commission of the applicability of such

subclause to the library. Such notice shall certify that the library in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the library is applying for funds under this subsection.

(F) Noncompliance

(i) Failure to submit certification: Any library that knowingly fails to comply with the application guidelines regarding the annual submission of certification required by this paragraph shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

(ii) Failure to comply with certification: Any library that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse all funds and discounts received under this subsection for the period covered by such certification.

(iii) Remedy of noncompliance

(I) Failure to submit: A library that has failed to submit a certification under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the library shall be eligible for services at discount rates under this subsection.

(II) Failure to comply: A library that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the library shall be eligible for services at discount rates under this subsection.

