

Children's Internet Protection Act Fact Sheet for Public Libraries

The Texas State Library contracted with the College of DuPage to bring Texas library staff a free workshop on CIPA and Web filtering. This workshop was broadcast at various host sites in Texas on March 12th, 2004. To inquire about viewing a videotape of that presentation, contact Anne Ramos (aramos@tsl.state.tx.us, 512-463-5494) or visit <http://www.tsl.state.tx.us/ld/workshops/teleconferences/videotapes.html> to learn more.

[download a copy of this document as a PDF](#)

What is the Children's Internet Protection Act?

In a nutshell, the Children's Internet Protection Act requires public libraries to install Internet filtering software on all of its computers (public access and staff) if the library uses federal money to purchase computers that will access the Internet or to purchase Internet access. In addition, libraries that receive an E-Rate discount for internal connections or Internet access must comply with CIPA.

Brief History

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 in April 5, 2001. In March 2001 several groups, including the American Library Association (ALA) and the American Civil Liberties Union (ACLU), filed suit to prevent the enforcement of CIPA's filtering requirement in public libraries. A trial was held in March 2002 in federal district court in Philadelphia. On May 31, 2002, the CIPA filtering mandate for public libraries was declared unconstitutional on first amendment grounds by the district court. The U.S. Justice Department appealed the district court's decision to the U.S. Supreme Court. On June 23, 2003, the Supreme Court announced its decision to overturn the May 2002 decision and uphold the Children's Internet Protection Act (CIPA).

The two "pockets" of federal money that are affected by this legislation are:

1. [E-Rate \(Universal Services\)](#) and;
2. LSTA ([Library Services & Technology Act](#))

More detailed guidance from the experts at the American Library Association, Universal Service Administrative Company and Institute of Museum & Library Services can be found using the hyperlinks in the [More Information](#) section below.

Under what conditions is CIPA compliance necessary?

E-Rate:

First, I encourage you to go to the Schools and Libraries Division (SLD), a division of the Universal Services Administrative Company (USAC), web site to view the Eligible Services List.

<http://www.sl.universalservice.org/reference/eligible.asp>

This list is divided into 3 major categories: Telecommunications, Internet Access, and Internal Connections. Services under Telecommunications are EXEMPT from CIPA compliance. Examples of Telecommunications Services include basic phone service, T-1, ISDN, Cable Modem, and DSL.

1. If your library receives the E-Rate discount on **Telecommunications Services ONLY**, then compliance with CIPA is **NOT** required.
2. If your library receives the E-Rate discount on even one item or service under Internal Connections or Internet Access, then your library **MUST** comply with CIPA.

LSTA:

1. Your library must comply with CIPA if your library uses LSTA money to purchase:
 - a. One or more PCs that will access the Internet; or
 - b. Internet access (i.e. pay an Internet Service Provider)
2. No compliance to CIPA is required if your library uses LSTA funds for ANY other purpose.

What is CIPA compliance?

If your library uses the E-Rate or LSTA funds in a manner that requires compliance as described above, then your library must:

1. Install and enforce the use of a technology protection measure* (i.e. filter) on every computer in the library with Internet access (public & staff).
*a technology protection measure must “protect” users from visual depictions – the blocking of objectionable text is not covered by the legislation. However, most filters block based on keywords or text. More information on "[technology protection measure](#)" below.
2. Adopt and enforce an Internet Safety Policy that includes the use of a technology protection measure. For E-Rate applicants, that Internet Safety Policy must meet the additional requirements as set forth in the Neighborhood Children’s Internet Protection Act (NCIPA)**
****NCIPA is a subtitle of CIPA; NCIPA only affects E-Rate applicants**

Libraries will be asked to certify CIPA compliance for the E-Rate and/or LSTA programs. A library which uses LSTA funds in a manner requiring CIPA compliance and does NOT receive a discount on Internet Access or Internal Connections through the E-Rate will need to certify compliance through the LSTA program. A library, which receives the E-Rate discount on Internet Access or Internal Connections, will certify compliance on a Form 486. A library, which uses both E-Rate and LSTA funds in a manner which requires CIPA compliance, will certify compliance on a Form 486 and then indicate that compliance to the LSTA program administrator. The certification documents for E-Rate and LSTA will have certification statements similar in nature to the following:

1. This public library has already complied with the Children's Internet Protection Act. (see [What is Compliance?](#) above)
2. This public library is undertaking action to comply with the Children's Internet Protection Act (see "[undertaking actions](#)" below)
3. This public library does not need to comply with the Children's Internet Protection Act because we do not use or plan to use the funds for services which would require CIPA compliance. (see [Under what conditions is CIPA Compliance Necessary?](#) above)

4. (LSTA Only) This public library has certified CIPA compliance under the E-Rate program because we receive the E-Rate discount on services requiring compliance.

NCIPA requirements:

1. An Internet Safety Policy must address the following items:
 - a. Access by minors to inappropriate matter on the Internet and the Web;
 - b. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
 - c. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
 - d. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
 - e. Measures designed to restrict minors' access to materials harmful to minors.
2. The Internet Safety Policy must be adopted after holding at least one public hearing or meeting. The law and the regulations give libraries considerable flexibility in meeting the public hearing mandate. The law says simply that 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.

When is the compliance deadline?

E-Rate:

The compliance deadline varies depending on a library's previous E-Rate application experience. A library that is asking for the E-Rate discount on Internet Access or Internal Connections for the very first time has one year to come into compliance (i.e. by July 1st of the next year). If Funding Year 2005 is the first year that a library requests the E-Rate discount on Internet Access or Internal Connections, then that deadline would be July 1, 2006. If Funding Year 2006 is the first year that a library requests the E-Rate discount on Internet Access or Internal Connections, then that deadline would be July 1, 2007.

Libraries not already in compliance may use the one year timeframe to undertake actions to come into compliance (i.e. develop an Internet Safety Policy; install and enforce the use of a technology protection measure). See below for more information regarding "[undertaking action](#)" and see above for "[What is compliance?](#)".

On a Form 486, where Internet Access or Internal Connections have been requested, libraries must certify compliance or that they are "undertaking action" to be in compliance by July 1st of the appropriate year. For example, if filing for Funding Year 2005 the deadline is July 1, 2006.

Following are a few examples of documentation that could demonstrate that a library is "**undertaking action**" to comply with CIPA:

1. A published or circulated library board agenda with CIPA compliance cited as a topic.
2. A circulated staff meeting agenda with CIPA compliance cited as a topic.
3. A Service Provider quote requested and received by a recipient of service or Billed Entity which contains information on a Technology Protection Measure.

4. A draft of an RFP or other procurement procedure to solicit bids for the purchase or provision of a Technology Protection Measure.
5. An agenda or minutes from a meeting open to the public at which an Internet Safety Policy was discussed.
6. An agenda or minutes from a public or nonpublic meeting of a school or library board at which procurement issues relating to the acquisition of a Technology Protection Measure were discussed.
7. A memo to an administrative authority of a library from a staff member outlining the CIPA issues not addressed by an Acceptable Use Policy currently in place.
8. A memo or report to an administrative authority of a library from a staff member describing research on available Technology Protection Measures.
9. A memo or report to an administrative authority of a library from a staff member which discusses and analyzes Internet Safety Policies in effect at other libraries.

This list is not meant to be exhaustive.

Some common questions regarding the Form 486 certification:

Q) I am about to file a Form 486 and I am NOT receiving a discount on anything except Telecommunications Services. What do I need to do?

A) Certify on your Form 486 that no compliance is necessary.

Q) I originally applied for and received a funding commitment for services that included Internet Access or Internal Connections. This library will not be installing a technology protection measure, what should I do?

A) You can submit your Form 486 accepting the discount for any Telecommunications Services requests that were funded. Services under this category do not require CIPA compliance. You would simply not accept the discount for those services which would require CIPA compliance. You would not include those funding requests on your Form 486. If you already included those services on a Form 486, you can CANCEL that request using a Form 500. Libraries that will not be "undertaking actions" to come into compliance and are not currently in compliance are NOT eligible for the E-Rate discount on Internet Access or Internal Connections.

Q) If the Billed Entity "applies" only for Telecommunications Services, would that situation constitute the Administrative Authority's First Funding Year for the purpose of CIPA?

A) No. A library who is a recipient of service is considered to have "applied" for funds in a Funding Year only when Form 486 for a Funding Request for Internet Access or Internal Connections has been successfully data entered. Since the Billed Entity "applied" only for Telecommunications Services in this situation, the Administrative Authority's First Funding Year was NOT established by the Funding Request in THIS Form 486.

More Frequently Asked Questions can be found at CIPA and the Form 486:
<http://www.sl.universalservice.org/reference/CIPAFaq.asp>

LSTA:

On August 1, 2003, the Institute of Museum and Library Services (IMLS) announced that Program Year

2004 of the Library Services and Technology Act funds would be the first to be affected by the public library requirements under the Children's Internet Protection Act. In Texas, the Program Year 2004 funds were distributed beginning September 1, 2004. Public libraries which are not already in compliance with CIPA must certify when applying for LSTA Program Year 2004 funds to purchase Internet Access and/or Internet Access computers that they are undertaking efforts to comply by the following year. Refer to the list above for examples of "undertaking action".

What is a technology protection measure?

Filtering or blocking technology restricts access to Internet content through a variety of means. Two basic types of filters currently dominate the market: filters that block content containing disapproved words (keyword blocking) and filters that block access according to a list of disapproved sites (site blocking). In either case, the filter manufacturer, in its own way and according to its own standards, determines which words or sites will be blocked. To comply with CIPA, a technology protection measure must "protect" users from visual depictions – the blocking of objectionable text is not covered by the legislation. However, most filtering solutions block based on keywords or text.

The choice of which technology protection measure to implement is a local decision.

Congress requested a study of technology protection measures from NTIA - National Telecommunications and Information Administration, US Department of Commerce. That study is available on the [NTIA website](http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/index.html) at <http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/index.html>

More Information:

[American Library Association](#)

CIPA Web site from ALA includes a FAQ for legal questions

Children's Internet Protection Act (CIPA)

http://www.fcc.gov/wcb/universal_service/chipact.doc

The Universal Service Administrative Company (USAC) administers the Universal Service Fund (USF), which provides communities across the country with affordable telecommunication services.

<http://www.sl.universalservice.org/reference/>

Institute of Museum & Library Services (IMLS) is a federal grant-making agency that administers the Library Services and Technology Act and the Museum Services Act (LSTA).

http://www.ims.gov/whatsnew/leg/protection_act.htm

E-Rate Central – dedicated to simplifying the E-Rate Program for Schools, Libraries and Vendors:

<http://www.e-ratecentral.com>

FAQ on E-rate Compliance with CIPA by Bob Bocher, Technology Consultant

Division for Libraries, Technology, and Community Learning -- Wisconsin Department of Public Instruction

www.dpi.state.wi.us/dltcl/pld/cipafaq.html

Read the FCC Order regarding compliance for Library E-Rate applicants:

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-188A1.txt

Filtering & filtering software:

<http://www.tsl.state.tx.us/ld/pubs/filters/filtering.html>

The National Telecommunications and Information Administration (NTIA) is an agency of the U.S. Department of Commerce. NTIA has released a [Report to Congress](#) mandated by the Children's Internet Protection Act of 2000 (CIPA). <http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/index.html>

Sample Internet Safety Policy:

<http://www.tsl.state.tx.us/ld/consulting/tech/isp2003.doc>

This sample policy was developed as a component of the workshop series “How to Develop an Effective Internet Safety Policy”. This workshop series has been offered in several locations across the state. In this sample, you will find commentary and suggestions to point out some of the areas that are dependent on local community need. The areas that are highlighted need specific attention. The bracketed information is commentary and suggestions, and would need to be removed from the actual policy your library creates.

For more information, please contact:

mjohnson@tsl.state.tx.us

512 463-5465