

CIPA Compliance Documentation Checklist

Current Funding Year	Checklist Completed By	Date Completed
----------------------	------------------------	----------------

Applicants that receive E-rate discounts for services other than basic telephone service (things like Internet Access, Internal Connections, or Basic Maintenance of Internal Connections) must certify on the Form 486 that they are in compliance with the requirements of the Children's Internet Protection Act. This checklist provides a guide for applicants to ensure that they have the documentation necessary to show compliance.

The Requirements of CIPA

CIPA requires that each applicant have the following:

1. A Technology Protection Measure

- That blocks or filters Internet access that protects against:
 - Access by adults and minors to visual depictions that are obscene, child pornography, or harmful to minors.
 - The measure may be disabled for adults engaged in bona fide research or other lawful purposes.
 - For schools, must also include the monitoring of the online activities of minors.

2. An Internet Safety Policy, which addresses:

- Access by minors to inappropriate matter on the Internet and WWW
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized and unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors

3. Public Notice and Hearing

- The applicant must hold at least one public hearing to address the proposed technology protection measure and Internet safety policy
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized and unlawful activities by minors online



CIPA Compliance Documentation Checklist

Demonstrating Compliance

Attaching the following documents to this checklist can help helpful to an applicant to demonstrate compliance with the requirements of CIPA:

Technology Protection Measure (TPM)

- Name of software/device used as a TPM:

 - A copy of a 'screen shot' of the TPM's 'About' window, showing Version/Revision Number
 - A copy of a 'screen shot' of the TPM showing that it is regularly updated with latest software updates, filter definitions, etc.
 - A report from the TPM showing Internet requests which were blocked
 - Copies of invoices and cancelled checks paid to vendors showing that the applicant has purchased the TPM and/or subscription to updates
 - Product documentation about the TPM that describes how it blocks content (URL based, keyword based, rating based, etc.)
-

Internet Safety Policy

- Copy of the Internet Safety Policy that addresses the items in #2, above
 - Date the attached Internet Safety Policy went into effect:

 - Additional policy/procedure documentation which describes how minors' online activities are monitored
 - Copy of public meeting agenda (board meeting, hearing etc.) where Internet Safety Policy and Technology Protection Measure were discussed
 - Copy of approved public meeting minutes where Internet Safety Policy and Technology Protection Measure were discussed
-

Notes

