E-Rate Central

CIPA Compliance Checklist

Schools and libraries that plan on receiving E-rate discounts on Internet access and/or internal connection services after July 1, 2002, need to be in compliance with the Children's Internet Protection Act ("CIPA"). CIPA compliance means that schools and libraries are filtering their Internet services and have implemented formal Internet Safety Policies (also frequently known as Acceptable Use Policies).

The Federal Communications Commission ("FCC"), charged with administering CIPA for E-rate purposes, has established only the broadest guidelines for interpreting the filtering and policy requirements of the Act. The following checklist is designed as a simple, but unofficial, guide for determining whether a school or library meets the CIPA compliance guidelines.

Internet Filtering:

Basic Requirement: 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." Filtering is required for all Internet-enabled computers whether used by minors or adults. For E-rate purposes, filtering for adult Internet usage can be disabled for "bona fide research or other lawful purpose."

Filtering Provisions	Yes (Y) or No (N)	Comments – Including filtering product name, if known.
Filtering is incorporated with the service provided by the Internet Service Provider.	No	
Filtering is provided locally for all Internet-enabled computers on a networked basis.	Yes	PaloAlto PA850 & GoGuardian
Filtering is provided individually on each Internet-enabled computer.	Yes	PaloAlto PA850 & GoGuardian

CIPA compliance requires a "Y" in at least one of the Filtering Provision boxes listed above.

Internet Safety Policy:

Basic Requirement: CIPA requires the public adoption and enforcement of an "Internet Safety Policy" covering the filtering discussed above. For minors, the policy must also address monitoring of online activities, the safety and security of all forms of direct electronic communications, unauthorized online access, and unauthorized disclosure of personal identification information.

Policy Provisions	Yes (Y) or No (N)	Comments
Filtering will be provided for all Internet-enabled computers used by students, patrons, and staff.	Yes	
Filtering will be disabled only for bona fide research or other lawful purposes.	Yes	
Online activities of minors will be monitored for appropriate use.	Yes	Monitored by BARK & GoGuardian
Safe and secure use by minors of direct electronic communications (including e-mail, chat rooms, and instant messaging) will be assured.	Yes	External emails are heavily restricted for students via Google Quarantine
Unauthorized online access, including "hacking" and other unlawful activities, is prohibited.	Yes	
Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is prohibited.	Yes	
The Policy was adopted with reasonable public notice and after at least one public meeting or hearing.	Yes	Meeting Type: Public___ Meeting Date: July 15, 2024

CIPA compliance requires a "Y" in all of the Policy Provision boxes listed above.

Additional information on Internet Safety Policy requirements and provisions can be found in the CIPA policy primer available on the E-Rate Central Web site at http://e-ratecentral.com/help/cipa_policy_primer.pdf.

Checklist Completed By:

Printed Name: Colton Shaver_____

Title: Director of Technology_____

Signature: _Colton Shaver_____

Date: __June 11, 2024_____

Checklist Completed By:

Printed Name: _____

Title: _____

Signature: _____

Date: _____