CIPA Compliance Checklist*

Must be completed and signed by two different staff members.

SCHOOL: Select School

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

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
2	Filtering will be provided for all Internet-enabled computers used by students, patrons, and staff.		
3	Filtering will be disabled only for bona fide research or other lawful purposes.		
4	Minors will be educated, supervised, and monitored with regard to safe and appropriate online activities.		
5	Safe and secure use by minors of direct electronic communications (including e-mail, chat rooms, and instant messaging) will be assured.		

6	Unauthorized online access, including "hacking" and other unlawful activities, is prohibited.		
7	Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is prohibited.		
8	The Policy was adopted with reasonable public notice and after at least one public meeting or hearing.		Form of Dissemination (e.g., Mtg., Website) _____ Date of Dissemination:_____

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

*Reference - E-Rate Central's CIPA Compliance Checklist (http://e-ratecentral.com/CIPA/default.asp). Additional information on Internet Safety Policy requirements and provisions can also be found in the *CIPA Policy Primer* available on the E-Rate Central Website.

The sections below have been added by the Catholic Schools Office.

9 **Student Email Accounts:**

Elementary schools are advised **NOT** to establish student email accounts. Although the login for some programs like Office 365 must follow the format of an email address, an actual email account is not required for students to utilize the program. (Emails are not required to access Google Classrooms.)

☐ **YES,** we have school established student email accounts for students in grades _____.

☐ **NO**, we do not have school established student email accounts.

Schools should have one of the following provisions in place for email:

- Email is filtered in-house, either by a dedicated email filtering appliance, email filtering software, or by an Internet filtering appliance or firewall confirmed to provide email filtering.
- Filtering is incorporated with the service provided by the Email Service Provider.
- Email is hosted by a cloud-based email provider (e.g., G Suite for Education, Office 365) AND filtering has been procured from another provider (e.g., Gaggle).

10 **Acceptable Use Policies for Students, Teachers, Staff, and Volunteers -** found in *Polices for Catholic Schools in the Diocese of Erie* (Policy 202.2 Acceptable Use of Internet, Computers and Network Resources). Agreements must be signed annually for ALL Students, Teachers, Staff, and Volunteers for Compliance.

☐ YES, Acceptable Use and Internet Safety Policy Agreements are on file for ALL Students, Teachers, Staff, and Volunteers.

11 ☐ We acknowledge that we are responsible for providing students annual instruction about **Digital Citizenship** and must keep a log and record of these activities on file at the school.

Checklist Completed By:

Printed Name: _____

Title: _____

Signature: _____

Date: _____

Checklist Certified By:

Printed Name: _____

Title: _____

Signature: _____

Date:_____

Complete annually and send a copy to the Catholic Schools Office by emailing (catholicschools@eriercd.org) by the date listed on MyDioErie 6b. > Back to School Forms & Information