Guidelines for a CIPA Compliant
Internet Safety Policy

Purpose
The purpose of this document is to assist in insuring that CIPA and NCIPA federal guidelines are observed and increase the likelihood that available funding can be acquired and maintained for all school districts that qualify for E-Rate and other technology related grants and reimbursement programs.

Background
In December of 2000 Congress passed the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA) as part of a large appropriations measure. The CIPA section of the appropriation deals directly with the internet filtering requirements established and the need for an Internet Safety Policy, while the NCIPA section addresses the specific elements that must be addressed within the Internet Safety Policy itself. For purposes of this text, the term CIPA will be used to include both CIPA and NCIPA requirements as a complete policy outlining internet safety procedures. This document focuses primarily on the CIPA requirements as they relate to the public school environment and compliance with the E-Rate program. In April of 2001, the Federal Communications Commission (FCC) issued regulations for CIPA.

Requirements

-Technology Protection Measure (Filter)
Schools must certify on their form 486, in the E-Rate application process, that they are in CIPA compliance by having an Internet Safety Policy adopted and implemented at the start of service of the given funding year. This policy must include a Technology Protection Measure that blocks or filters internet access to visual depictions that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors.

Schools subject to CIPA must also maintain a policy in which the online activities of minors are monitored.

-Internet Safety Policy
Schools subject to CIPA are required to adopt a policy that addresses:
1. Access by minors to inappropriate matter on the internet
2. The safety and security of minors when using electronic mail, chat rooms, and other
   forms of direct electronic communications
3. Unauthorized access including "hacking" and other unlawful activities by minors online
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors
5. Restricting minors' access to materials harmful to minors

-Public Meeting with Reasonable Public Notice
Schools subject to CIPA must hold a public hearing in which the Technology Protection Measure (filtering process) and the proposed Internet Safety Policy are both addressed.

Considerations and Exceptions

Acceptable Use Policy
Many of the safeguards contained in the above CIPA requirements are common to an Acceptable Use Policy that may already be in place for a particular school district. If the current AUP adopted and implemented by a school district meets **all** the requirements stated in the CIPA legislation, then that AUP, by strict definition, will contain a CIPA compliant Internet Safety Policy.

I would caution those considering using your current AUP as a CIPA compliant policy, to carefully review the details contained in the CIPA legislation and make certain they are adequately addressed in the AUP. We have observed otherwise very complete AUP documents not pass the scrutiny of federal audit when CIPA components are closely examined.

In some instances, an amendment to the existing AUP might suffice. In other situations it might be best to draft a new stand alone document that clearly outlines the specific CIPA requirements head on.

It should be noted that when submitting an Internet Safety Policy as part of your Technology Plan you should only submit the CIPA required elements if contained within an existing AUP and not the entire AUP or the entire school handbook.

Compliance Needed or Exceptions Granted
CIPA compliance is needed when applying for E-Rate discounts that request "Internet Access" and/or "Internal Connections" (This includes ICN consortium members)
CIPA compliance is not required when applying for E-Rate discounts requesting "Telecommunication" services only

CIPA compliance is needed when using Title II-D Enhancing Education through Technology, or Library Services and Technology Act grant funds for purchasing computers that access the internet.
CIPA compliance can be waived in your first funding year of E-Rate as long as you certify that you are "undertaking actions" to comply with CIPA. The details and required documentation for this exception are located at the following link:
http://www.universalservice.org/sl/applicants/step10/cipa.aspx

Local Considerations
Aside from the federal CIPA requirements the FCC leaves many of the internet use requirements to reside under local control measures identified in the school district's Acceptable Use Policy.

Remember that the CIPA language outlines the elements that will be "addressed" and not necessarily prescribed or prohibited in certain instances. Recognizing that no internet filtering solution is 100% effective, the Technology Protection Measure must "protect" against the visual depictions identified by federal law but not "prevent" those same visual depictions without fail. This point is significant in understanding that there is no FCC endorsed or prescribed filtering technology.

Filtering must be in place for all computers with internet access. This includes computers accessed exclusively by staff and those computers made available to the public.

The filtering can take place at the ISP, WAN, LAN, or PC level depending on the needs of the individual school or district.

Filtering or blocking measures may be disabled during use by an adult to enable access for bona fide research or other lawful purposes.

While e-mail, chat rooms and other internet services must be addressed it is within local control to determine whether or not there might be an educational application to this type of communication in controlled classroom conditions.

Monitoring of the online activity of minors is required but CIPA does not require the tracking or logging of internet use by minors or adults.

In many instances the majority of school districts, if not fully compliant with CIPA requirements, are most likely in need of a minor amendment to an existing internet policy that is currently in place. Providing the district has addressed the details in implementing a Technology Protection Measure (Filter), Internet Safety Policy, and a Public Meeting with Reasonable Public Notice to review the policy, they will be CIPA compliant.

For the purposes of E-Rate, CIPA compliance is certified when filing the form 486 for a given funding year. It is good practice however to maintain a copy of board minutes and the relevant agenda outlining Internet Safety Policy review and adoption.