CIPA and eRate Compliance

Frequently Asked Questions & Best Practice Guidance

The Children's Internet Protection Act (CIPA), enacted December 21, 2000, requires recipients of federal technology funds (eg. eRate) to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act ("NCIPA") which addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act, enacted October 10, 2008, adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

CIPA Frequently Asked Questions*

What is CIPA?

The Children's Internet Protection Act is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program.

Who is considered a minor?

Any individual who has not attained the age of 17 years.

Do schools have to implement filtering technology to be compliant?

CIPA requires the implementation of a "technology protection measure" to block access to certain *visual depictions*. The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to *visual depictions* that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. **HARMFUL TO MINORS**, meaning any picture, image, graphic image file, or other visual depiction that:
   a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
   b. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact (the meanings given such terms in section 2246 of title 18, United States Code.) , actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
   c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

*Excerpts of this document taken from http://e-ratecentral.com/CIPA/

Can that "technology protection measure" be removed for adults/staff?

Yes, there is a specific exception for instances when bona fide research requires the filter to be turned off.

Are schools required to block social networking sites based on CIPA?

No, the FCC has established that social network websites (eg. Facebook) do not fall into one of the categories that are required to be blocked. That said, there is a provision for each organization to block additional categories that are deemed inappropriate for minors by local standards.

What about the Internet Safety Policy?

CIPA requires the adoption and enforcement of an Internet Safety Policy (ISP) covering the filtering requirements as well as addressing "monitoring the online activities of minors" and appropriate online behaviors. Monitoring does not require a technology though Districts can use technology to monitor the online activities of students. Monitoring can also simply refer to adult supervision (eg. classroom management). The Protecting Children in the 21st Century Act says that as of July 2012 an E-Rate recipient's Internet Safety Policy "Must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response."

Internet Safety Policy Development

What does a strong Internet Safety Policy look like?

- Leave as little to interpretation as possible but just enough room for compromise and common sense analysis of unique situations.
- Create the brightest line possible between the responsibilities of the student, the teacher, the school, and the parents. The days where a teacher who is properly managing students can be reprimanded for the transgression of a single student in their class should be over.
- The policy should also address how classrooms with technology components are laid out, in order to facilitate the highest level of classroom management for teachers and staff.
- Use a public meeting to understand the concerns of the community. Use surveys prior to drafting the Acceptable Use Policy (AUP) and then gather information needed to finalize the draft during the meeting itself.
- List what you block and describe the process by which you can request or question blocking.
- Say what you do and do what you say.

Where does your Internet Safety Policy end and Acceptable Use Policy begin?

- ISP is more overarching and refers to the federal law, while the AUP is a local district level policy and is different for staff and students. For example, it's not against the law for a teacher to play Angry Birds on their lunch break using a work computer,

but if the AUP says it's against the rules of the institution, then it becomes a problem.

Enforcing network policy while protecting student's constitutional rights

- There needs to be differentiation between the First Amendment right of a student and what is acceptable use on school grounds during school hours.
- There is an assumption of privacy, even on school grounds, particularly when dealing with personal items belonging to the student. There is a limit to the level of inspection and intrusion and crossing it can have significant fiscal and public image impacts.
- Policy and procedure must set a limit to the actions of teachers, administrators, and districts to mitigate the risk of lawsuits or damaging complaints. For example, if a student is seen using a personal device to access inappropriate content, the device may be confiscated but staff should refrain from looking at any data contained on the phone because it is still considered the property of student.

Training

- Any staff or faculty member that is qualified to teach students, can become qualified to teach CIPA-mandated content. Because there is no benchmark for exactly what the content is or how it should be delivered, staff or faculty could be trained to understand the policy, and can develop a curriculum for students. This training could be from any reliable and qualified source that your curriculum department deems appropriate.
    - Be aware of any contractual requirements and/or district-employee relations issues that may impact attempts to comply with CIPA training.
- There are many private sector providers of CIPA compliance services but care should be taken to select a reputable vendor. Many less scrupulous vendors have made less than accurate claims in their advertisements.

Community meeting

- Announce the meeting in his many public media sources as possible. Examples would be district and school websites, printed newsletters to parents, e-mail announcements, or any other widely available means to communicate with parents and community members.
    - It is a best practice to describe the background of the issue, and provide information about where parents and stakeholders can further educate themselves prior to the public meeting. A copy of the pending AUP (or a link to it) should also be included.
- At the meeting itself, minutes should be taken and/or the meeting itself should be recorded. It is particularly important in the event that USAC asks for proof that the meeting occurred.

- Release a survey either on on both paper and email in order to gather information on the initial concerns of the public. This can give valuable insight as to the thoughts of the community in relation to technology acceptable use.

Practical CIPA Management

Governance

Most school districts currently filter web content in some shape or form. However CIPA requirements are broad enough to possibly require an increase in the level of filtering that occurs. Bearing that in mind it is worth considering a governance structure to help technology departments adapt these to the broader district goals and needs. Below are listed some ideas to consider surrounding governance. These are drawn from existing, demonstrated practice by other school districts from across the nation:

- Open control of filtering practice beyond the technology department
  - Form a committee structure to routinely review filtering needs and provide overall oversight
  - Involve other key stakeholders from across the district:
    - teachers, administrators, district technologists, librarians, media specialists, and parents
- Meet on regular basis to reassess both needs, requirements, and technologies used
    - Have a review process for filters to meet changing times and needs
    - Think about how filtering certain content areas could affect the classroom (e.g., games, shopping, weapons, etc.)
- Develop administrative regulations or board policy to help provide official process structure around filtering, why it is done, and how to request changes
- Post list of content categories that are filtered and make it available and easy to find online
- Allow for time-limited manual overrides by teachers (if possible) to help ease classroom frustration
- Consider how to provide protection beyond the district owned desktop/laptop
  - Mobile devices
  - Personal computers on district property
  - Home computers

Violations

It is a violation of CIPA to not have adequate technology measures in place to block prescribed visual depictions. It is not a violation if a student views those prescribed visual depictions at school on a website, internet search or other method either because it was outside the filter by accident or because the student willfully sought a way around the filter (e.g. proxy site). Filtering technology is not fool-proof. It is also a violation to not have monitoring of internet traffic/activity by students. This can be a technology or adult supervision in learning environments. Districts should have a policy and stick to it.

*Excerpts of this document taken from http://e-ratecentral.com/CIPA/