

Maine School Administrative District #75 Internet Safety Plan

Introduction. The District has taken reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. However, on a public network, it is impossible to control all materials. While the list of "blocked" sites is updated continually via subscription, it is nearly impossible to list all inappropriate sites.

The teacher/staff will choose resources on the Internet that are appropriate for classroom instruction and/or research for the needs, maturity and ability of their students. The District takes no responsibility for the accuracy or quality of information from Internet sources. Use of any information obtained through the Internet is at the user's risk.

Requirements. The Children's Internet Protection Act (CIPA) has three requirements.

1. Technology Protection Measure (Filtering)
2. Internet Safety Policy
3. Public Meeting on the Internet Safety Policy

To comply with these requirements the District has a technology protection measure in place, a board adopted Acceptable Use Policy, and has provided public meetings on the policy.

Technology Protection Measure (Filtering). The District utilizes SurfControl Web Filter for Novell BorderManager. The system is regularly updated to ensure the maximum protection is available from the vendor. A separate Internet Monitoring system provided by SurfControl tracks Internet usage and potential problem areas with the filters. SurfControl's integrated solution for Novell BorderManager allows a network administrator to configure outgoing rules for Internet filtering the CyberLISTs, a listing of well researched Internet sites. Requests from network workstations that are directed to the BorderManager server for Internet access are checked against these outgoing rules before access is allowed. Inappropriate sites that are accessed because they are not on the SurfControl list are manually added to the system and reported to SurfControl via the "Submit-a-site" tool found at <http://www.surfcontrol.com/>

SurfControl provides content filtering based on 40 customizable categories identifying nearly 2.4 Million Domains, covering 689 Million web pages. A BorderManager login screen challenges access to inappropriate sites. Student users are not provided with additional Internet privileges and cannot bypass security features. Staff users have additional but not full access to all blocked Internet content after entering their NDS account information. Log files are rotated weekly and are retained for four weeks. Each log file is analyzed by software with statistics published for network administrator review. BRDSTATS.EXE provides a simple analysis tool that includes a html format report including top URL list, top URL analysis, top users, hourly traffic analysis, weekly traffic analysis, top proxy server return codes, top file types, file size analysis, and a summary. Users are identified only if they logged in to BorderManager during a session. Users who do not log in are identified as "Unknown User". The log file does identify unknown users by IP address. DHCP makes it possible to match an IP Address to a workstation. SurfControl's non-integrated solution offers all the added benefits of the latest version of SurfControl control including Real-Time monitoring and notification, expanded categories, detailed reports, and Precision Bandwidth Control, using SurfControl's patented Pass-By Technology for Windows NT/2000. All Internet activity is monitored by the system.

Internet Safety Policy. The policy is available online at <http://www.link75.org/helpdesk/techplan/policyacceptable.pdf>

Public Meeting on the Internet Safety Policy. A district wide meeting regarding the policy was held at Mt Ararat Middle School. Additional public meetings were held and televised on public access television regarding the policy during the policy approval process during several school board meetings. Subsequent meetings and notices regarding the policy and the status of the technology protection measures are a routine practice.

Law (<http://www.maine.gov/msl/erate/filtering/cipafa01-2.htm>). *“The law states that **all** computer workstations that can access the Internet must have some type of blocking or filtering technology in place. (In the law this is known as a "technology protection measure.") **This includes student, staff, administrative, and patron workstations accessed by minors or adults.** Under certain circumstances there is a provision that allows filters to be disabled as described in the next question.”*

“The law states that an administrator, supervisor, or other authorized person may disable the filter to allow Internet access for lawful purposes. (Note: Even without CIPA, there is no constitutional protection to allow viewing of obscene pictures, and child pornography, regardless of its medium, is clearly illegal.)“

“The law does not give a person the right to have filtering disabled, rather it gives permission to authorized school or library staff to disable the filter for lawful purposes.”

The law requires filtering of visual depictions of

- 1. obscenity,*
- 2. child pornography, and*
- 3. materials harmful to minors (minors only).*

The law does not require the filtering of text.

These terms are defined in the act as follows:

- 1. "Obscenity" is defined in a reference to section 1460 of title 18, U.S. Code*
- 2. "Child pornography" is defined in a reference to section 2256 of title 18, U.S. Code*
- 3. "Harmful to minors" is defined in CIPA and means any picture, image, graphic image file, or other visual depiction that, with respect to minors:*
 - a. taken as a whole, appeals to a prurient interest in nudity, sex, or excretion;*
 - b. depicts, describes, or represents, in a patently offensive way, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and*
 - c. taken as a whole, lacks serious literary, artistic, political, or scientific value.*