

**STUDENTS AND INSTRUCTION** **5000**

INTERNET ACCESS NETWORK 5500

GUIDELINES FOR PUBLISHING ON [www.melroseschools.com](http://www.melroseschools.com) 5503

The purpose of the melroseschools.com web site is to further the goals of the Melrose Public Schools, by

- improving communication among the administrators, staff, students, parents and other community members, and
- by giving students and staff an opportunity to practice the skills required to publish their work on the web.

All material published on the web site should be appropriate to the educational purpose of the site, consistent with district policies, and of such quality as to reflect positively on the school system and community.

- Submissions should always be checked for correct spelling and grammar.
- Announcements and other calendar information should be accurate and timely, and obsolete entries should be removed promptly.
- Privacy rules (defined below) shall be strictly followed.
- Student essays and other “opinion” pieces should be clearly labeled as such and should be appropriate to the site.
- Inappropriate content is strictly forbidden. Inappropriate content includes any content that is defamatory, abusive, obscene, vulgar, sexually explicit, threatening, harassing, racially offensive, illegally discriminatory, or otherwise illegal.
- External links should be to sites that are consistent with the educational purpose of this site. Specifically forbidden are links to: student personal sites; entertainment sites; game sites; as well as sites which would be deemed inappropriate as defined above.
- Copyright material may only be used with the permission of the owner. This applies to images as well as text.

**Privacy** of community members must be protected at all times. Personal information about students, staff and volunteers, should only be posted under the following conditions:

- The parents of every student in the Melrose Public Schools are asked to return a media release form at the beginning of each school year. On this form, they are asked to indicate whether they give permission for the *name* and *image* of the student to appear on the web site. Student names and recognizable likenesses may only be placed on the web site if a signed media release form is on file in the principal’s office of the student’s school.
- Other contact information for students may *not* be placed on the web site under any circumstances. This includes street address, phone number, and email address. Links to student web pages on other servers are also strictly forbidden.
- Staff members may be identified by name, and information on how to contact them at school may be listed (including school address, phone number and email address).
- Contact information for adult volunteers and other community members and additional contact information for adult staff (such as personal email) may be listed with the permission of the party in question.

Responsibility for the site ultimately rests in the hands of the central administration staff, and, in particular, with the Director of Technology. Portions of the site may be delegated, at the Director's discretion, to individual responsible adult "webmasters". These webmasters will in some cases develop and publish content themselves, while in other cases they will monitor the contributions of others, including students. At the discretion of the Director, students may be given access to the site, but only under the direct and active supervision of an adult supervisor or sponsor. In such cases, the student will be expected to follow these guidelines, and the supervisor will be expected to monitor the student's work to ensure this compliance. *Potential supervisors should only request access (and accounts) for their students if they are confident in their ability to monitor their students' activities.* In no case will a student be given access to publish on the web site without some responsible adult advisor.

Every person given access to the web site will receive a personal user id and password from the Director of Technology or his staff. This id and password should never be "loaned" to another individual: instead, an additional id should be requested. This process encourages the confidentiality of passwords and enables the administration to keep track of submissions by author. *Users will be held responsible for all actions performed by sessions associated with their user ids.*

Statewide standards for format and content are intended to facilitate navigation between parts of the site and to enable viewers of the site to communicate with the site administrators when necessary. To this end, all pages should follow these rules:

- Directory and file names should use only lower case letters, digits, underscore and dot characters.
- Pages should use standard file suffixes (.htm or .html)
- Every directory that contains *any* pages should contain an index page named index.html. This index page should follow the linkage conventions described below. Note that directories containing only image or other similar data need *not* include an index page.
- Every page that contains *any* navigable links should contain at least one "up" link to the index page for its directory or a parent directory. Every index page should contain a link to the main index page (href"/index.html") for the melroseschools.com site. It is recommended that *every* page have such an uplink; however, it is permissible to use "leaf" pages that contain no references at all. This exception is allowed primarily to make it easier to publish data by converting it (eg, from Word files) without requiring hand editing to create uplinks.
- Every page should have a descriptive page title and heading.
- Every page should contain a footer including the following information: date last modified, identity of person or organization responsible for the page, and a mailto: link to this responsible party. Organization names should be used whenever appropriate, to maintain the privacy constraints outlined above. (eg, "This page maintained by the Melrose Middle School PTO" rather than "This page maintained by Vincent Volunteer").
- Pages that express individual student opinions should include a disclaimer, eg. "The views represented on this page are those of the author and do not necessarily represent those of the Melrose Public Schools".

# Children's Internet Protection Act Policy and Guidelines Melrose Public Schools

Superintendent of Schools: Dr. Charles Martin  
Director of Information Technology: Dr. Reza Namin

## Overview

***“The Children’s Internet Protection Act (CIPA) was signed into law on December 21, 2000. Under CIPA, no school or library may receive discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology (see below). This Internet Safety Policy must protect against access, through computers with Internet access, to visual depictions that are obscene, child pornography, or (in the case of use by minors) harmful to minors. The school or library must also certify that it is enforcing the operation of such filtering or blocking technology during any use of such computers by minors. The law is effective for Funding Year 4(07/01/2001 to 06/30/2002) and for all future years. Schools and libraries receiving only Telecommunications Services are excluded from the requirements of CIPA.***

For the first Funding Year (07/01/2001 to 06/30/2002), Melrose Public Schools certified on the Form 486 that are undertaking actions to put into place an Internet Safety Policy and to procure the filtering or blocking technology. For the second year (07/01/2002 to 06/30/2003) has certified on their Form 486 that are in compliance with CIPA in order to receive universal service discounts.

Appropriate certification for “undertaking actions”

Melrose Public Schools certify that, as of the date of the start of discounted services, Melrose Public Schools pursuant to the Children’s Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (1), are undertaking such actions, including any necessary procurement procedures, to comply with the requirements of CIPA for the Year 5 finding year (07/01/2002 to 06/30/2003).

Compliance with the requirements of CIPA

“Undertaking such actions” refers to actions related to implementation of the CIPA requirements that should be in place for Year 5. These requirements are:

### 1. Technology Protection Measure

Melrose Public Schools is taking variety of Technology Protection Measures such as monitoring the online activities of minors as well as the purchasing and use of Cyber Patrol Software and its services and Watch Guard that blocks or filter Internet access. In addition a state of art filtering and firewall services is provided by MEC Merrimack Education Center). The Technology Staff at Melrose Public Schools Continue to monitor

## BACKGROUND

1. Pursuant to section 254 of the Act, the Federal Communications Commission (Commission) established the schools and libraries universal service support mechanism (colloquially known as the “e-rate” program). Under that mechanism, eligible schools, libraries, and consortia that include eligible schools and libraries (collectively, recipients), may apply for discounted eligible telecommunications, Internet access, and internal connections services.
2. The Schools and Libraries Division (SLD) of the Universal Service Administrative Company (Administrator) administers the schools and libraries support mechanism under the direction of the Commission. After an applicant for discounted services under the schools and libraries support mechanism has entered into agreements for eligible services with one or more service providers, it must file with SLD an FCC Form 471 application. The Form 471 notifies the Administrator of the services that have been ordered, informs the providers with whom the applicant has entered into an agreement, and supplies an estimate of funds needed to cover the discounts to be given for eligible services. SLD then issues a finding commitment decision letter indicating the discounts, if any, to which the applicant is entitled. The approved recipient of discounted services subsequently submits to SLD an FCC Form 486, which triggers the process for SLD to receive invoices from the service provider.
3. CIPA amends, *inter alia*, section 254 of the Act to impose new requirements on schools and libraries “having computers with Internet access” and receiving discounted services under the schools and libraries universal service support mechanism. Specifically, under CIPA, no school or library may receive universal service discounts unless the authority with responsibility for administration of the school or library makes the required certifications, and ensures the use of such computers in accordance with the certifications. They must certify that they are enforcing a policy of Internet safety and have in place a technology protection measure. The policy of Internet safety must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are (1) obscene, or (2) child pornography, or, with respect to use of the computers by minors, (3) harmful to minors. The entity must also certify that its policy of Internet safety includes monitoring the online activities of minors. CIPA does not, however, require the tracking of Internet use by any identifiable minor or adult user. Furthermore, CIPA requires that recipients provide reasonable public notice and hold at least one public hearing or meeting to address this proposed policy of Internet safety.

### **Selecting and disabling the “technology protection measures”**

Under CIPA, a “technology protection measure” is narrowly defined as follows:

“The term ‘technology protection measure’ means a specific technology that blocks or filters internet access to visual depictions that are: (a) obscene, as that term is defined in section 1460 of title 18, United States Code; (b) child pornography, as that term is defined in 2256 of title 18, United States Code; or (c) harmful to minors.”

The Federal Communications Commission (FCC) did not identify which filtering products, if any, complied with CIPA and instead ruled that local communities are the correct authorities to make this decision.

Schools receiving covered eRate support cannot disable the filters when minors are using them, even with parental or teacher permission and supervision.

Appropriate school staff may disable filters only for adults who are using school computers for “bona fide research purposes.” The FCC also declined to further define bona fide research, noting: “We leave such determinations to the local communities, whom we believe to be most knowledgeable about the varying circumstances of schools and libraries in those communities.”

The process for monitoring students' internet use also was left to local decision-making. The rule makes clear that schools are not required to use electronic monitoring and data collection to satisfy the monitoring requirement.

“Obscenity” is defined as any picture, image, graphic image file, or other visual depiction that: (1) taken as a whole appeals to a prurient [i.e. erotic] interest; (2) depicts, describes or represents in a patently offensive way an actual or simulated sexual act or sexual contact or a lewd exhibition of the genitals; AND (3) taken as a whole lacks serious literary, artistic, political, or scientific value. 18 U. S.C. § 1460.

“Child Pornography” is defined as any visual depiction. . . whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—(1) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (2) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct; (3) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (4) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct. 18 U.S. C. § 2246.

“Harmful to Minors” is defined as:

Any picture, image, graphic image file, or other visual depiction that (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) 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, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. *See, e.g.,* 47 U.S.C. § 254 (1) (1) (a) (v). Federal-State Joint Board on Universal Service: Children’s Internet Protection Act; 66 Fed. Reg. 19394 *et seq.* (April 16, 2001) (to be codified at 47 CFR part 54.520). Federal-State Joint Board on Universal Service: Children’s Internet Protection Act; 66 Fed. Reg. 19394 *et seq.* (April 16, 2001) and use variety of filtering devices to protect against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with Internet access by minors - harmful to minors. This measure may be disabled for adults engaged in bona fide research or other lawful purposes.

## 2. Internet Safety Policy

The Internet Acceptable Use and Safety Policy at Melrose Public Schools address the following issues:

- a. access by minors to inappropriate matter on the Internet and World Wide Web;
- b. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- c. unauthorized access, including so-called “hacking,” and other Unlawful activities by minors online;
- d. unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- e. measures designed to restrict minors’ access to materials harmful to minors.

## 3. Public Notice and Hearing

The Information Technology Department with guidance of Dr. Reza Namin, the Director of Information Technology will provide reasonable public notice and hold at least one public hearing to address a proposed Technology Protection Measure and Internet Safety Policy.

Documentation for “undertaking actions”

Melrose Public Schools will maintain all appropriate documentation and information in its files for audit purposes. An undertaken action is an action which can be documented and which moves the Melrose Public Schools toward compliance.

Following are a few examples of documentation that demonstrate that Melrose Public Schools is “undertaking actions” to comply with CIPA:

- a. A published or circulated Melrose Public Schools agenda with CIPA compliance cited as a topic.
- b. A circulated staff meeting agenda with CIPA compliance cited as a topic.
- c. A Service Provider quote requested and received which contains information on a Technology Protection Measure.
- d. A draft of an RFP or other procurement procedure to solicit bids for the purchase or provision of a Technology Protection Measure.
- e. An agenda or minutes from a meeting open to the public at which an Internet Safety Policy was discussed.
- f. An agenda or minutes from a public or nonpublic meeting of a school or library board at which procurement issues relating to the acquisition of a Technology Protection Measure were discussed.
- g. A memo to an administrative authority of Melrose Public Schools from a staff member outlining the CIPA issues not addressed by an Acceptable Use Policy currently in place.
- h. A memo or report to an administrative authority of Melrose Public Schools from a staff member describing research on available Technology Protection Measures.
- i. A memo or report to an administrative authority of Melrose Public Schools from a staff member which discusses and analyzes Internet Safety Policies in effect at other schools and libraries.

Whose Access Must Be Filtered?

As a general rule, Melrose Public Schools block or filter all access to “visual depictions” that are obscene, child pornography, harmful to minors, or that the Melrose Public Schools authority determines are “inappropriate for minors.” (Text is not affected.) This law applies to both minors and adults, although adults are not restricted in their access to “harmful [or] inappropriate for minors” materials.

The question of whether and when to disable filters to access material requested by a library patron or a student is one that will require careful consideration. The CII’A bill contains several provisions addressing the issue of a library or school administrator disabling filtering software “to enable access for bona fide research or other lawful purposes.” Those institutions that receive funding from more than one of the covered programs face conflicting requirements. The entire bill requires certification that the school, “is enforcing the operation of such technology protection measure during any use of such computers by minors.” The phrase “any use” is repeated in describing the requirements for filtering adult use of the Internet. However, a later portion of the Title III and LSTA sections reads:

**DISABLING DURING CERTAIN USE:** An administrator, supervisor, or person authorized by the responsible authority under paragraph (1) may disable the technology protection measure concerned to enable access for bona fide research or other lawful purposes.”

The exception for disabling filters in the E-Rate section of the bill differs:

**DISABLING DURING ADULT USE:** An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

A “minor” is defined as persons under 17 years of age, meaning that different requirements may apply to a school or library based on students’ ages as well as the source of program funds.

MSC first vote 8/14/07

MSC second vote 8/28/07