

INTERNET SAFETY

This Internet Safety Policy is a supplement to our current Instructional Network Acceptable Use Policy. The Internet Safety Policy is to clarify issues pertaining to filtering and Internet monitoring for the users of the network and to be in explicit compliance with the Children's Internet Safety Act (2001).

Filtering: The Dedham Public Schools maintains a single point of access to the Internet through a central connection to an Internet Service Provider. At this access point a filtering system is maintained to block material inappropriate to children. Among the items filtered are visual depictions that are obscene, child pornography, or material harmful to minors.¹ It should be noted that due to the nature of the Internet no filtering system is perfect. The DPS subscribes to a service that provides a preliminary list of blocked sites that are regularly updated. The Dedham Public Schools has the ability to add additional blocked sites or to remove sites we find to be inappropriately blocked.

Monitoring: The teacher or staff member supervising the child has the primary responsibility of monitoring the Internet for student safety and appropriate use. Students are prohibited from using a computer without direct supervision of a teacher or staff member. The DPS network has a monitoring system to record Internet sites accessed. The technology staff reviews this list periodically.

Messaging: Messaging includes posting items such as text to a bulletin board, discussion group, use of email, and "chat" features including instant messaging. Students are prohibited from using messaging except within the password protected, web-enhance Intranet classroom between the teacher and the students enrolled in an individual class. Additionally, teacher-sponsored email accounts for groups such as the high school newspaper journalists and those that maintain the Dedham Public Schools website are allowed. These accounts are under the direct supervision of an assigned teacher. The Dedham Public Schools maintains the right to monitor all messaging on its system.

Responsibility: Each user and his/her parent/guardian must have signed the Instructional Network Acceptable Use policy. Each user must take responsibility for his or her use of the computer network and Internet and avoid inappropriate sites. If a student finds that other student users are visiting offensive or harmful sites, he/she should report such use to the supervising staff member.

Identification of Students on the Web: Student work published on the web by children under age 18 will not be identified by his/her last name.

Security: The Dedham Public Schools provides a secure network for the school community. As stated in the Instructional Network Acceptable Use Policy, hacking attempts or other illegal activities are monitored and strictly prohibited.

¹ The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h] [7]), as meaning any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, on actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Confidentiality of Student Information: Personal information concerning Dedham Public Schools students will not be disclosed or used in any way on the Dedham Public Schools web site without the specific permission of a parent or guardian or if the student is age 18 or over, the student. Users are strongly discouraged from providing private or confidential information about themselves or others on the Internet. The school administration may authorize the release of student information, as defined by state law, for internal administrative purposes or approved educational projects and activities.

Recommendations for the home:

Personal Safety for Children: When using the Internet do not reveal personal information such as your name, home address or phone number or any information that might allow a person to locate you. Never agree to meet a person that you “meet” on the Internet face-to-face without your parent’s permission and without an adult being present. If someone attempts to arrange a meeting with you through the Internet, you must report this communication to your parent or guardian. Instant messaging should not be used at home unless explicitly approved by and supervised by parents. Screen names should be chosen carefully (e.g. Soccer_Kicks is better than Pretty Sally13). Never phone an online ‘acquaintance’ without parental permission, caller ID can trace a phone number and from that the address can be found. Do not reply to harassing, threatening or sexual messages and report any such communication to the police.

Filtering at home: There are a number of filtering programs that allow parents to block sites and monitor a child’s use of the Internet including the time of day, number of hours and types of access such as chat, web, or newsgroup activities. It is recommended that parents use this type of filtering if their child will use the Internet without direct parental supervision. Filtering can be set to restrict all Internet use when parents are not home. For more information refer to <http://www.getnetwise.org/> and <http://www.safekids.com/>

Location of Computer: Place the computer in a heavy traffic area in the home. The best place for a home computer used by a child is in an area such as the living room or kitchen while the worst place is a child’s bedroom.

Parent - Child dialog: Encourage constant dialog with your child about what they are doing online. Have your child show you what they are doing. Consider an acceptable use policy for the home.

Violations: The Internet has much value in today’s world and is available in many public places including our libraries. Try to establish consequences that use violations as a teachable moment rather than “pulling the plug” on all home Internet access.

Reporting: Report illegal or suspicious contact with your child to appropriate law enforcement and/or Cybertipline (1-800-843-5678) or <http://www.cybertipline.org>. If a child is in danger, call the police.

Approved by School Committee April 16, 2008