

INTERNET SAFETY/INTERNET CONTENT FILTERING POLICY

A. Introduction

1. In compliance with the Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the District has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students.
 - a) **Obscene:** The term "obscene" is defined, pursuant to New York State law, as any visual depiction that average person applying contemporary community standards would find that, taken as a whole, it appeals to the indecent interest, that depicts in a patently offensive way actual or simulated: sexual intercourse, criminal sexual act, sexual bestiality, masturbation, sadism, masochism, excretion or lewd exhibition of the genitals and that, taken as a whole, lacks serious literary, artistic, political or scientific value.
 - b) **Child pornography.** The term "child pornography" is defined, pursuant to CIPA, as any visual depiction, including any photography, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
 - i. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
 - ii. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or
 - iii. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
 - c) **Harmful to minors.** The term "harmful to minors" is defined, pursuant to CIPA, as any picture, image, graphic image file, or other visual depiction that:
 - i. Taken as a whole and with respect to minors, appeals to a indecent interest in nudity, sex, or excretion;
 - ii. 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
 - iii. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
2. The District will provide for the education of students regarding appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response. Further, the Director of Educational Technology and Information Systems shall enforce the operation of the technology protection measure during any use of District computers and ensure compliance with this policy by monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with internet access. He or she shall also be responsible for ensuring that staff and students receive training on their requirements.

3. Further, the Board of Education's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate teaching/instructional materials and activities to enhance the schools' programs; and to help ensure the safety of personnel and students while online.
4. However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate material. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.
5. In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web *may* include, but shall not be limited to, the following guidelines:
 - a) It shall be the responsibility of staff members to supervise minors when using the online computer network and access to the Internet, including the use of electronic mail, chat rooms, instant messaging and other forms of direct electronic communications. As determined by the Director of Technology and/or his/her designee, the use of email, as well as social networking websites, may be blocked as deemed necessary to ensure the safety of such students;
 - b) Monitoring logs of access in order to keep track of the websites visited by students as a measure to restrict access to materials harmful to minors;
 - c) In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and
 - d) Appropriate supervision and notification to students regarding the prohibition as to unauthorized disclosure, use and dissemination of personal identification information regarding minors.
6. The determination of what is "inappropriate" for minors shall be determined by the District and/or designated school official(s). It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research.
7. Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable shall only be exercised by the Director of Technology and/or his/her designee
8. The District shall provide certification, pursuant to the requirements of CIPA, to document the District's adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking/filtering of access to certain material on the Internet) for all District computers with Internet access as well as its monitoring the online activities of minors.

B. Internet Safety Instruction

1. In accordance with New York State Education Law, the District may provide, to students in grades K through 12, instruction designed to promote the proper and safe use of the Internet. The Commissioner shall provide technical assistance to assist in the development of curricula for such course of study which shall be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.
2. Under the Protecting Children in the 21st Century Act, students will also be educated on appropriate online behavior, including interactions with other individuals on social networking websites and in chat rooms, as well as cyberbullying awareness and response. Such instruction shall be provided even if the District prohibits students from accessing social networking sites or chat rooms on District computers.

C. Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

1. Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events.
2. The District is not responsible for inappropriate content or material accessed via a student's own personal technology or electronic device or via an unfiltered Internet connection received through a student's own personal technology or electronic device. However, the use of personal technology or electronic devices by students on school property or at school functions must be in accordance with the District's Technology Use Policy and Code of Conduct. Students who are found to be accessing inappropriate content or material on personal technology or electronic devices on school property or at school functions may be subject to appropriate discipline.

D. Notification/Authorization

1. The District's Technology Use Policy will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet.
2. The District has provided reasonable public notice and has held at least one (1) public hearing or meeting to address the proposed Internet Safety/Internet Content Filtering Policy prior to Board adoption. Additional public notice and a hearing or meeting is not necessary when amendments are made to the Internet Safety Policy in the future.
3. The District's Internet Safety/Internet Content Filtering Policy must be made available to the FCC upon request. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of this policy as well as any other District policies relating to the use of technology.
4. The Internet Safety/Internet Content Filtering Policy is required to be retained by the school for at least five (5) years after the funding year in which the policy was relied upon to obtain E-rate funding.

47 USC Sections 254(h) and 254(l)
47 CFR Part 54
Education Law Section 814

REF: Policy #4526 – Technology Use Policy
Policy #5300 – Mahopac Central School District Code of Conduct
Adoption Date : March 12, 2013