

Menno School District	NEPN Code: JFCE(IIBH)
Policy Manual	

Internet Safety Policy (CIPA)

Introduction

The Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5), and South Dakota Consolidated Statutes Section 22-24-55 require public schools to implement certain measures and actions to ensure that students are restricted from accessing inappropriate materials online using school-owned computers.

In order to comply with this requirement the Menno School District shall: 1) restrict access by minors to inappropriate matter on the Internet, 2) provide for the safety and security of minors when using email, chat rooms and other forms of direct electronic communications, 3) guard against unauthorized access, including hacking and other unlawful activities by minors online, 4) guard against unauthorized disclosure, use and dissemination of personal identification information regarding minors, 5) provide measures designed to restrict minors' access to materials harmful to minors, and 6) provide education to students concerning online safety.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications and access to inappropriate information on school computers.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to inappropriate matter such as child pornography, obscene material and material that is harmful to minors. Adult users may request that the technology protection measures be temporarily disabled in order to conduct bona fide research or for another lawful purpose. The technology protection measures must be re-activated as soon as the adult finishes using the computer for the authorized bona fide research or other lawful purpose. The district uses the firewall/filtering device or application currently provided by the state. The district purchases the companion product to provide off-site filtering.

Safety and Security

To the extent practical, steps shall be taken to protect computer users from harassment and unwanted or unsolicited electronic communications when using electronic mail, chat rooms, and other forms of direct electronic communications. The district uses the state provided email or another email provider with the ability to apply filtering to messages. Other electronic communications are with the staff supervision.

Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator.

Unauthorized Access

It is the responsibility of all users to ensure that a safe, secure network exists. So called "hacking" or other unlawful activity will not be tolerated. Any user, student or adult, with knowledge of such activity shall report it to the Technology Coordinator or School Administrator. Users found participating in such activity shall be reprimanded according to school policy.

Dissemination of Personal Information

At the beginning of each school year network users shall be required to complete and sign an acceptable use policy. This will include authorizing the use of certain personal information, picture, and school work in school online media. Network users are prohibited from disclosing such information without proper authorization.

Supervision and Monitoring

It shall be the responsibility of all members of the Menno School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator or designated representatives.

The Technology Coordinator shall be responsible for monitoring the current network filtering device to ensure that it is working correctly. Any changes in filtered categories will be discussed with administration. Individual sites may be unblocked only if they are proved to be of particular educational value to an individual or shown to have been incorrectly categorized. Updating of any blocking/filtering software will be at the advice of the state.

Education Component

The school district will educate students annually concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The Superintendent is delegated authority to implement these educational requirements and report annually to the Board on the educational activities undertaken to comply with this section.

Additionally, information about technology use is provided to parents during orientation meetings held at the beginning of the year in conjunction with freshmen participation in our 1:1 project. Information also may be provided during certain PTA functions and during Parent/Teacher Conferences.

Discussion includes school filtering as well as home filtering, internet safety and general use of technology.

Definitions

Minor: The term “minor” means any individual who has not attained the age of 17 years.

Obscene: The term “obscene” is defined as material – (1) the dominant theme of which, taken as a whole, appeals to the prurient interest; (2) which is patently offensive because it affronts contemporary community standards relating to the description or representation of sado-masochistic abuse or sexual conduct; and (3) lacks serious literary, artistic, political, or scientific value.

Child pornography: The term “child pornography” is a visual depiction, including any photograph, 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 the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 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 such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Harmful to minors: The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that—(i) taken as a whole and with respect to minors, appeals to a prurient 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.

Technology protection measure: The term “technology protection measure” means a specific technology that blocks or filters Internet access to the material that is obscene, contains child pornography and/or is harmful to minors.

Computer: Any electronic device that has the ability to connect to the Internet including but not limited to desktop computers, laptop computers, tablet computers and electronic book readers.

Adopted: 6-11-12