

6081.20 Internet Safety Policy. The District utilizes technical and instructional measures to provide a positive, productive educational experience for all users, in order to comply with the requirements of the Children’s Internet Protection Act (CIPA) and the Neighborhood Children’s Internet Protection Act (NCIPA). No filters are 100% effective. To the extent practical, filters are used on all Internet-enabled computers to block or filter electronic communications and access to inappropriate information for both minors and adults.

- A. Filters automatically eliminate protocols that are not consistent with District Rules and Regulations and protect against Internet access to visual depictions that are:
 - 1. “*Obscene*: This is defined in a reference to Section 1460 of Title 18, U.S. Code.
 - 2. *Child pornography*: This is defined in a reference to Section 2256 of Title 18, U.S. Code, or
 - 3. *Harmful to minors*: This is defined in CIPA and means any picture, image, graphic image, file, or other visual depiction that:
 - 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 conduct, 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.”
- B. Procedures to temporarily disable filtering for “adults only” for “bona fide research or other lawful purpose” are in place.
- C. Pursuant to the Children’s Internet Protection Act (CIPA, 12-21-2000), the Superintendent and designees have established procedures to maximize system safety and security and, to the extent practical, to prevent inappropriate network usage, including, but not limited to:
 - 1. “The prevention of user access to, or transmission of, inappropriate material over its computer networks, via Internet, electronic mail, or other direct electronic communications;
 - 2. the prevention of unauthorized access and other unlawful online activity, such as hacking,
 - 3. the prevention of unauthorized on-line disclosure, use, and dissemination of personal information regarding minors, and
 - 4. the use of dissemination of personal identification information of minors.”
 - 5. Students and parents are required to read and sign the Student Responsible Use Contract before students are allowed access to the network.
 - 6. Each student who receives a network account will receive instruction from a Moscow School District staff member pertaining to the proper and responsible use of the District’s networks and the Internet.
- D. District staff is responsible for instructing students in:
 - 1. Use of appropriate strategies when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications to ensure their safety and security,
 - 2. Unauthorized access, including so-called “hacking” and other unlawful activities by minors online, such as vandalism and harassment,
 - 3. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors,
 - 4. Search strategies designed to restrict minor’s access to materials harmful to minors (local standards prevail),
 - 5. Copyright and plagiarism,
 - 6. Downloading files.

- E. District staff is responsible for supervising and monitoring online activities. An information literacy curriculum provides students with the understanding and skills needed to use electronic resources effectively, and in an appropriate and responsible manner. District staff is responsible for integrating the use of technology into curriculum activities. District network staff monitors and evaluates sites not currently categorized or that might be categorized incorrectly. District administrators will make determinations on an as-needed basis as to whether specific uses of the network are consistent with acceptable use practices. (6-23-09)

6081.20.01 Content Publishing Guidelines.

- A. No personal information about a student will be allowed. This includes but is not limited to home telephone numbers and addresses, as well as information regarding the specific location of any student at any given time.
- B. Only initials may identify individuals in pictures, movies, or sound recordings. Absolutely no use of first and last names may appear in reference to individuals in pictures, movies, or sound recordings.
- C. No full-faced photos may be used. (6-23-09)

This Internet Safety Policy was adopted by the Board of Trustees at a public meeting following normal public notice on June 23, 2009.