

The Board of Education recognizes the value of the internet and the worldwide web for instructional purposes. While unable to guarantee complete safety the Board is committed to protecting students from internet sites harmful to minors. To this end, the Board directs the Superintendent of Schools or his designee to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to depictions that are obscene, and
- minors to depictions that are obscene, or harmful to minors, as defined in the Children's Internet Protection Act.

These protections may be disabled or relaxed for students and staff conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or a designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet. The Superintendent or designee shall establish and implement procedures that enforce these restrictions.

The computer network coordinator designated under the district's Computer Network or Acceptable Use Policy, shall monitor all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

Proposed June 2002

Approved June 2002

Reviewed June 2004