



(X) Required
 () Local
 () Notice

INTERNET SAFETY POLICY

The Board of Education is committed to undertaking efforts that serve to make safe for students the use of district computers for Internet access. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

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

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or 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 Instructional Technology Manager designated under the district's Computer/Network Acceptable Use (4526-E) shall monitor and examine 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, 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 policy on the acceptable use of computers and the internet (Policy 4526). Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

Ref: Public Law No. 106-554
 47 USC §254
 20 USC §6801

Adoption date: July 9, 2007
 Revision date: June 15, 2021