

INTERNET SAFETY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of District computers for access to the Internet, World Wide Web and Intranet. 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 pornographic, and
- minors to visual depictions that are obscene, pornographic, violent, or harmful to minors, as defined in the Children’s Internet Protection Act.

Any such measures may not be disabled or relaxed for adults conducting research or other purposes.

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 the event that the District applies for E-rate funds, it will certify that is educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

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, World Wide Web and Intranet. 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 and examine all District computer network activities to ensure compliance with this policy and accompanying regulation. They 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, World Wide Web, and Intranet, 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.

Access and/or use of the Internet, World Wide Web, and Intranet through personal devices outside of the District’s computer network, but while on District grounds, must also comply with this policy and regulations as well as the Code of Conduct. Failure to do so may result in disciplinary action pursuant to the Code of Conduct, or, for employees, pursuant to applicable disciplinary procedures under law or collective bargaining agreements.

Ref: Public Law No. 106-554; 47 USC §254; 20 USC §6801
Adopted: June 21, 2006
Revised: November 2, 2011
Reaffirmed: April 8, 2015