INTERNET SAFETY

The Board of Education is committed to undertaking efforts that serve to protect students who use district computers to access the Internet and World Wide Web. 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 his or her 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 including monitoring the online activities of students using district computers and restricting student access to materials that are obscene, inappropriate and/or 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 and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Technology, or other designee of the Superintendent shall monitor and examine all district computer network activities to ensure compliance with this policy. 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, in addition to generally accepted rules of network etiquette, and the district’s Acceptable Use Policy and Regulation. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

The District shall provide age-appropriate instruction regarding appropriate online behavior, including: (1) interacting with the other individuals on social networking sites and in chat rooms; and (2) cyberbullying awareness and response. Instruction will be provided even if the district prohibits students from accessing social networking sites and/or chat rooms on district computers.

This Policy also incorporates the Board’s Acceptable Use Policy and Regulation, including, but not limited to, the provisions regarding the district’s use of technology protection measures, the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications and prohibited user conduct, including the unauthorized disclosure, use and
dissemination of personal information regarding students and unauthorized online access (“hacking”) by students, as well as access by students to inappropriate matter on the Internet and World Wide Web.

Cross-Ref: Acceptable Use Policy No. 4526
Acceptable Use Policy Regulations No. 4526-R

Ref: Children’s Internet Protection Act, Public Law No. 106-554
    Broadband Data Services Improvement Act/Protecting Children in the 21st Century Act, Public Law No. 110-385
    47 USC §254
    20 USC §6801

Adoption date: April 29, 2008
Revised: June 12, 2018
Reviewed: October 29, 2019