Internet Safety

The Board of Education is committed to efforts that serve to make internet use safe for children. 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\(^1\), 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 digital 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 and World Wide Web (collectively “Internet”). The Superintendent or designee shall establish and implement procedures that enforce these restrictions.

The Technology Director designated under the District’s Computer Network or Responsible Use for Technology and the Internet Policy, 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. The district shall also provide age appropriate instruction to students regarding appropriate online behavior including but not limited to interacting on social networks, websites and chat rooms, and cyberbullying awareness and response. Such instruction will be provided even if the District prohibits students from accessing social networking sites and chat rooms on District Technology.

All users of the District’s technology resources, including access to the Internet, must understand that use is a privilege, not a right, and that any such use entails responsibility. Users must comply with the requirements of Federal and State laws and regulations, this policy, in addition to generally accepted rules of network etiquette, and the District’s Computer Network

---

\(^1\) Any picture, image, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, and actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

Adopted: June 27, 2012

Ref: Public Law No. 106-554 (Children’s Internet Protection Act)  
Public Law No. 110-384 (Protecting Children in the 21st Century Act)  
47 USC §254  
20 USC §6801  
Page 1 of 2
Systems Policy. Failure to comply may result in disciplinary action including but not limited to the suspension and revocation of technology access privileges; discipline in accordance with law and the District Code of Conduct for students, discipline in accordance with law and applicable collectively negotiated agreement for employees, as well as legal action where appropriate.