

Instruction

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY

District will use technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers and other electronic devices with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers and other electronic devices with Internet access by minors, considered harmful to such students. The District will provide for the education of students in the area of digital citizenship, including appropriate online behavior including interacting with other individuals on social networking Web sites in chat rooms, and regarding cyberbullying awareness. Further, appropriate monitoring of online activities of minors, as determined by the building/program supervisor, will also be enforced.

While no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations, proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web *may* include, but shall not be limited to, the following guidelines:

- a) The presence of a supervising teacher and/or other appropriate District personnel when students are accessing the Internet in school. As determined by the appropriate building administrator, the use of e-mail and chat rooms may be blocked as deemed necessary;
- b) Monitoring students' use of District owned computers and other electronic devices with internet access while they are on school grounds;
- c) The dissemination of the District's Acceptable Use Policy and accompanying Regulations to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet. Parental and/or student consent, as may be applicable, shall be required prior to authorization for student use of District computers. In compliance with this Internet Safety Policy as well as the District's

(Continued)

Instruction

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and

- d) Notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal information regarding such students.

Students should not expect that information stored on the District's computer system will be private. Parents/guardians are responsible for monitoring 1-1 device usage when the device is not in school. However, the District reserves the right to filter content and notify parents/guardians and take appropriate action in the event the content violates the District's Code of Conduct or District Policies.

The determination of what is "inappropriate" for minors shall be determined by the District and/or designated school official(s). It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measure," "sexual act," and "sexual contact" will be as defined in accordance with Children's Internet Protection Act (CIPA) and other applicable laws/regulations as may be appropriate and implemented pursuant to the District's educational mission.

47 United States Code (USC) Sections 254(h) and 254(l)

47 Code of Federal Regulations (CFR) Part 54

Adopted: October 13, 2020 By Lyncourt Board Of Education