Book	Policy Manual
Section	For Board Review - Vol. 34, No. 1
Title	STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	
Adopted	April 23, 2007
Last Revised	August 17, 2020

7540.03 - **STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY**

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning to incorporate the vast, diverse, and unique resources available through the Internet. The Board provides ~~T~~technology ~~R~~resources (as defined in Bylaw 0100 - Definitions) to support the educational and professional needs of its students and staff. With respect to students, ~~District~~ Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and Internet system do not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of ~~District~~ ~~T~~technology ~~R~~resources by principles consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of ~~District~~ Technology Resources and students' personal communication devices when they are connected to the District computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity (see Policy 5136 - Personal Communication Devices).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using ~~District~~ Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

The Board may not be able to technologically limit access to services through its ~~e~~Education ~~t~~Technology to only those that have been authorized for the purpose of instruction, study, and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures, that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measures may not be disabled at any time that students may be using the Education Technology if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Board utilizes software and/or hardware to monitor online activity of students and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

At the discretion of the Board or the Superintendent, the technology protection measure may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measure may not be disabled at any time that students may be using the Network, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act.

The Superintendent or designee may temporarily or permanently unblock access to websites or online education containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measure. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measure.

The Superintendent or designee may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Parents are advised that a determined user may be able to gain access to services on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents may find inappropriate, offensive, objectionable or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

The Superintendent is directed to prepare guidelines which address students' safety and security while using e-mail, chat rooms, and other forms of direct electronic communications, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking") and other unlawful activities by minors online.

Education t~~T~~echnology is provided as a tool for education. The ~~School~~ District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

Pursuant to Federal law, students shall receive education about the following:

A. the safety and security of students while using e-mail, chat rooms, social networking sites, and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online; and,

C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students or staff online;

D. unauthorized disclosure, use, and dissemination of personal information regarding minors.

Staff members shall provide instruction for their students regarding the appropriate technology use and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school. Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions, or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

~~Building~~ Principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the e~~E~~ducation t~~T~~echnology. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. All Internet users (and their parents if they are minors) are required to confirm their agreement to abide by the terms and conditions of this policy and its accompanying guidelines during the annual student registration process.

~~[Drafting Note: If the District participates in the Federal Universal Service E-Rate Program for Schools, the Federal Communications Commission (FCC) requires the following language be included in your acceptable use policy.]~~

~~[ ]~~ ~~Off~~ premises use of E-Rate supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

Students will be assigned a school email account that they are required to utilize for all school-related electronic communications, including those to staff members and encouraged to use with individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned email account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes. Students shall not use their school-assigned email account for non-school related electronic communications or to signup/or register for any non-school related mobile applications/apps.

Students and staff members are responsible for good behavior on the Board's e~~E~~ducation t~~T~~echnology just as they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the e~~E~~ducation t~~T~~echnology that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students shall not access social media for personal use from the District's network during the school day, but shall be permitted to access social media for educational use in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying guidelines may have their use privileges restricted or revoked, and disciplinary action taken against them. Users of the Board's e~~E~~ducation t~~T~~echnology are personally responsible and liable, both civilly and criminally, for uses of the e~~E~~ducation t~~T~~echnology not authorized by this Board policy and its accompanying guidelines.

The Board designates the Superintendent and the Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to the use of the District's e~~E~~ducation t~~T~~echnology.

Revised 9/19/11
Revised 3/18/13
Revised 3/14/16

Legal

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246

47 C.F.R. 54.500 - 54.523