Book	Policy Manual
Section	Tech III
Title	REPLACEMENT POLICY - SPECIAL UPDATE - INFO & TECH COLL. - PHASE III - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Number	po7540.03 ss 7-31-18
Status	Draft
Adopted	September 20, 2016
Last Revised	July 31, 2018

REPLACEMENT POLICY - SPECIAL UPDATE - INFO & TECH COLL. - PHASE III

7540.03 - **STUDENT TECHNOLOGY 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 School Board provides technology resources (as defined in Bylaw 0100) 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 technology 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 Code of Student Conduct. This policy and its related administrative procedures and the Code of Student 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).

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).

First, the Board may not be able to technologically limit access, through its technology resources, to only those services and resources 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 procedures 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 (CIPA). 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 Board also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using District technology resources, if such disabling will cease to protect against access to materials that are prohibited under the CIPA. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or District Network Manger/ Assistant Manager may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. 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 measures.

Parents are advised that a determined user may be able to gain access to services and/or resources 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.

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

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

B. the dangers inherent with the online disclosure of personally identifiable information;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students online; and,

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

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school.

[X] 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.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying procedures. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms, and cyberbullying awareness and response. All users of District technology resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures.

[X] Students will be assigned a school e-mail account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and ~~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 e-mail 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 are responsible for good behavior when using District technology resources - i.e., behavior comparable to that expected of students when 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 approve any use of its technology resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying procedures.

[NOTE: If language about social media is added to Policy 7540, it is recommended that this language be added to this policy.]

[X] Students may only use District technology resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying procedures may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District technology resources that are not authorized by this policy and its accompanying procedures.

The Board designates the Superintendent and District Network Manager/ Assistant Manager as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying procedures as they apply to students' use of District technology resources.

Legal	F.S. 1001.43
	F.S. 1001.51
	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. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
	20 U.S.C. 6777 (2003)
	20 U.S.C. 9134 (2003)
	18 U.S.C. 2256
	18 U.S.C. 1460
	18 U.S.C. 2246
	47 C.F.R. 54.500
	47 C.F.R. 54.501
	47 C.F.R. 54.502
	47 C.F.R. 54.503
	47 C.F.R. 54.504
	47 C.F.R. 54.505
	47 C.F.R. 54.506
	47 C.F.R. 54.507
	47 C.F.R. 54.508
	47 C.F.R. 54.509
	47 C.F.R. 54.511
	47 C.F.R. 54.513
	47 C.F.R. 54.514
	47 C.F.R. 54.515
	47 C.F.R. 54.516
	47 C.F.R. 54.517
	47 C.F.R. 54.518
	47 C.F.R. 54.519
	47 C.F.R. 54.520
	47 C.F.R. 54.522
	47 C.F.R. 54.523
Cross References	ap7540.03 - STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Last Modified by Sam Stalnaker on July 31, 2018