Book	Policy Manual
Section	Board Review 37.2 - Technology
Title	Vol. 37, No. 2 - Technology - February 2023 Revised STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	
Adopted	May 14, 2001
Last Revised	February 8, 2016

Revised Policy - Vol. 37, No. 2

7540.03 - **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology directly affects~~has fundamentally altered~~ the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt~~As a result, educators are continually adapting~~ their means and methods of instruction, and the way they approach student learning, to incorporate the latest technologies. The Board of Education provides Information & Technology Resources (as defined in Bylaw 0100) (collectively, "District Information & Technology Resources")~~vast, diverse, and unique resources available through the Internet. The Board of Education 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 Information & 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 does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its stated~~limited~~ educational purpose.

The Board regulates the use of District Information & Technology Resources in a manner~~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 Information & Technology Resources and students' personal communication devices when they are connected to District Information & Technology Resources, including online educational services/apps, regardless of whether such use takes place on or off school property~~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).

Students are prohibited from using District Information & Technology Resources to engage in illegal conduct (e.g., libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines and the Student Code of Conduct (e.g., making personal attacks or injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on students' First Amendment rights~~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 Information & Technology Resources are not unlimited, the Board may institute~~has also instituted~~ restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

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

While the Board uses various technologies to limit students using its Information & Technology Resources to only use/access online educational services/apps and resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent students from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members~~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 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) when significant portions of students' education take place online or through the use of online educational services/apps~~, 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 implements~~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 Information & Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under CIPA~~the Children's Internet Protection Act~~. Any student who attempts to disable the technology protection measures will be disciplined~~subject to discipline~~.

The Superintendent or Technology Director_____ may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been mistakenly, improperly, or inadvertently~~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 online content and/or services/apps ~~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 content~~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.

Principals are responsible for providing training so that students under their supervision are knowledgeable about this policy and its accompanying guidelines.

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 guidance and instruction to their students regarding the appropriate use of District Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not be limited to, education concerning appropriate online behavior including interacting with others on social media, including in chat rooms, and

cyberbullying awareness and response~~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 they are 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. ~~**[END OF OPTION]**~~

~~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 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 students who use~~users of~~ District Information & 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 guidelines. (See Form 7540.03 F1)

In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, students are required to comply with all District-established cybersecurity procedures ~~**( )** including, but not limited to, the use of multi-factored authentication for which they have been trained~~ **[END OF OPTION]**. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

[x] Students will be assigned a District-provided 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. **(x)** 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/apps~~, including mobile applications/apps that will be utilized by the student for educational purposes.~~ ~~**[END OF OPTION**~~]

Students are responsible for good behavior when using District Information & Technology Resources – i.e., behavior comparable to that expected of students when they are in physical classrooms and school buildings and at school-sponsored events. Because communications~~classrooms, school hallways, and other school premises and school-sponsored events. Communications~~ on the Internet are often public in nature, general~~. General~~ school rules for behavior and communication apply. The Board does not approve any use of its Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

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

[x] Students may only use District Information & 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. **[END OF OPTION]**

Users who disregard this policy and its accompanying guidelines 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 Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and _____Director of Technology Services as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Information & Technology Resources.

Legal

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

P.L. 110-385, Title II, Protecting Children in the 21st Century Act

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

47 C.F.R. 54.500 – 54.523

Last Modified by Chris Rice on April 12, 2023