



Book	Policy Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	Active
Legal	West Virginia State Board of Education policy 2460 – Education Purpose and Acceptable Use of Electronic Resources, Technologies, and the Internet P.L. 106-554, Children's Internet Protection Act of 2000 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003) 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003) 18 U.S.C. 1460 18 U.S.C. 2246 18 U.S.C. 2256 20 U.S.C. 6777, 9134 (2003) 47 C.F.R. 54.500 – 54.523
Adopted	April 2, 2007
Last Revised	December 6, 2016

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 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 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 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).

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 to services 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), 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.

The West Virginia Department of Education (WVDE), approved service provider, and other State agencies operate the Statewide infrastructure to provide Internet access for all Pre-K-12 public schools. Pursuant to Federal law, the State 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. Electronic filtering will be installed by the West Virginia Department of Education at the two (2) points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management. This service enables County/schools to meet the Children's Internet Protection Act (CIPA) and E-Rate guideline requirements for filtering.

The Board shall add other electronic filters at the local level.

With approval of the Board, schools may add other electronic filters at the local level.

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 Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such websites 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.

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 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 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 guidelines.

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 guidelines.

The WVDE reserves the right to monitor, inspect, investigate, copy, review, and store, without prior notice, information about the content and usage of any network and system files, user files, disk space utilization, applications, bandwidth utilization, document files, folders, electronic communications, e-mail, Internet access, and any and all information transmitted or received in connection with networks, e-mail use, and web-based tools.

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 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 Technology Resources that are not authorized by this policy and its accompanying guidelines.

Based upon the acceptable use and safety guidelines outlined in West Virginia Board of Education policy 2460, the State Superintendent, the WVDE and the WVNET system administrators will determine what is appropriate use, and their decision is final. Also, the system administrator and/or local teachers may deny user access at any time.

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted if and when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, United States Code <http://copyright.gov/title17>) and content is cited appropriately.

The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Technology Resources.

Revised 8/15/11

Revised 6/18/12

Revised 9/1/15

Revised 12/6/16

© Neola 2016