Book	Policy Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	Active
Adopted	October 6, 2011
Last Revised	January 22, 2025

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

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt 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") 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 educational purposes only and utilizes apps and services (as defined by Bylaw 0100) 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 stated educational purpose.

The Board regulates the use of District Information & Technology Resources in a manner 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 ("PCDS") when they are connected to District Information & Technology Resources, including apps/services, regardless of whether such use takes place on or off school property (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. Because its Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Students 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).

While the Board uses various technologies to limit students using its Information & Technology Resources to only use/access apps/services and other 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 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 apps/services.

Pursuant to Federal law, the Board implements 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 the 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. Any student who attempts to disable the technology protection measures will be disciplined.

The Superintendent or Technology Director may temporarily or permanently unblock access to websites or apps/services containing appropriate material if access to such sites has been mistakenly, improperly, or inadvertently 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 apps/services 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 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 ("PII") 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. Furthermore, staff members will monitor, in accordance with Federal and State law, the online activities of students while they are 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 District will provide parents with appropriate notice – to the extent required by State law – when such monitoring takes place.

All students who use 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. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Students will be assigned a District-provided school email account that they are required to use for all school-related electronic communications, including those to staff members, peers, individuals, and/or organizations outside the District with whom they are communicating for school-related projects and assignments.

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 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 Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

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.

Use of Artificial Intelligence Tools For School Work

To ensure the integrity of the educational process and to promote fair and equal opportunities for all students, except as outlined below, the use of Artificial Intelligence (AI) tools is strictly prohibited for the completion of school work. The use of AI tools, without the express permission/consent of a teacher, undermines the learning and problem-solving skills that are essential to academic success and that the staff is tasked to develop in each student. Students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI tools and they should ask their teachers when they have questions and/or need assistance. Unauthorized use of AI tools is considered a form of plagiarism, and any student found using these tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct.

Notwithstanding the preceding, students can use AI tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the AI tools in an ethical and responsible manner. Teachers have the discretion to authorize students to use AI tools for the following uses:

A. Research assistance: AI tools can be used to help students quickly and efficiently identify background information, including locating relevant information and sources for their school projects and assignments, suggesting research questions, providing opposing viewpoints, identifying blind spots, and suggesting other perspectives.

B. Data Analysis: AI tools can be used to help students with pattern identification and to analyze, understand, and interpret large amounts of data, such as text documents or social media posts. This can be particularly useful for research projects or data analysis assignments – e.g., scientific experiments and marketing research.

C. Language translation: AI tools can be used to translate texts or documents into different languages, which can be helpful for students who are learning a new language or for students who are studying texts written in a different language. AI tools can also remove abstract language from a text, adjust text complexity, and provide background information about a culture to help a student understand texts.

D. Writing assistance: AI tools can provide feedback on a student’s writing, including grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills. Similarly, AI tools can offer suggestions to modify tone and voice, organize a student’s thinking, identify bias, suggest additional topics, and ask questions to expand the student’s thinking on a topic.

E. Accessibility: AI tools can be used to help students with disabilities access and understand written materials. For example, text-to-speech software can help students with specific learning disabilities or visual impairments to read texts and AI-powered translation tools can help students with hearing impairments understand spoken language (e.g., create transcripts or provide closed-captioning for spoken material).

When AI tools are used responsibly and effectively, they can supplement, not replace, traditional learning methods. If a student has any questions about whether they are permitted to use AI tools for a specific class assignment, they should ask their teacher.

In accordance with their teacher’s direction, students are required to cite/identify work generated/created with the use of AI tools and explain/demonstrate how the AI tools were used in the creation of the work.

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 Technology Director 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.

Revised 8/2/12
Revised 5/16/16
Revised 6/29/23

© Neola 2024

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

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 C.F.R. 54.500 - 54.523

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

Cross References

po5500 - STUDENT CONDUCT

po7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

po7540.09 - ARTIFICIAL INTELLIGENCE ("AI")