

## 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 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 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 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 (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. 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 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 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.

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 online educational services/apps 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 services/apps 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:

- safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- the dangers inherent with the online disclosure of personally identifiable information;
- 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
- 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. Furthermore, staff members will monitor 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.

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 utilize 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. 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.

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.

## Use of Artificial Intelligence/Natural Language Processing Tools for School Work

Students are required to rely on their own knowledge, skills, and resources when completing school work. In order 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) and Natural Language Processing (NLP) tools (collectively, “AI/NLP tools”) is strictly prohibited for the completion of school work. The use of AI/NLP 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/NLP tools and they should ask their teachers when they have questions and/or need assistance. Unauthorized use of AI/NLP 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/NLP tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the AI/NLP tools in an ethical and responsible manner. Teachers have the discretion to authorize students to use AI/NLP tools for the following uses:

- Research assistance: AI/NLP tools can be used to help students quickly and efficiently search for and find relevant information for their school projects and assignments.
- Data Analysis: AI/NLP tools can be used to help students 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.
- Language translation: AI/NLP 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.
- Writing assistance: AI/NLP tools can provide grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills.
- Accessibility: AI/NLP 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.

As outlined above, under appropriate circumstances, AI/NLP tools can be effectively used as a supplement to and not a replacement for traditional learning methods. Consequently, with prior teacher permission/consent, students can use such resources to help them better understand and analyze information and/or access course materials. If a student has any questions about whether they are permitted to use AI/NLP tools for a specific class assignment, they should ask their teacher.

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 the 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.

STUDENT NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY AGREEMENT

To access e-mail and/or the Internet at school, students must obtain parent permission and must sign and return this form

**Use of the Internet is a privilege, not a right. The Board of Education’s Internet connection is provided for educational purposes only. Unauthorized and inappropriate use will result in a cancellation of this privilege.**

The Board has implemented the use of a Technology Protection Measure which is a specific technology that will protect against (e.g., block/filter) Internet access to visual displays that are obscene, child pornography or harmful to minors. The Board also monitors online activity of students in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. Nevertheless, parents/guardians are advised that determined users may be able to gain access to information, communication and/or services on the Internet which the Board has not authorized for educational purposes and/or which they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. Parents/Guardians assume this risk by consenting to allow their students to participate in the use of the Internet. **Students** accessing the Internet through the school's computers assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet.

The Board has the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the Board's computers/networks. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

**Please complete the following information:**

Student User's Full Name (please print): \_\_\_\_\_

Grade: \_\_\_\_\_

Parent/Guardian's Name: \_\_\_\_\_

**Parent/Guardian**

As the parent/guardian of this student, I have read the Student Network and Internet Acceptable Use and Safety Policy and Guidelines, and have discussed them with my child. I understand that student access to the Internet is designed for educational purposes and that the Board has taken available precautions to restrict and/or control student access to material on the Internet that is obscene, objectionable, inappropriate and/or harmful to minors. However, I recognize that it is impossible for the Board to restrict access to all objectionable and/or controversial materials that may be found on the Internet. I will not hold the Board (or any of its employees, administrators or officers) responsible for materials my child may acquire or come in contact with while on the Internet. Additionally, I accept responsibility for communicating to my child guidance concerning his/her acceptable use of the Internet - i.e., setting and conveying standards for my daughter/son to follow when selecting, sharing and exploring information and resources on the Internet. I further understand that individuals and families may be liable for violations.

To the extent that proprietary rights in the design of a web site hosted on the Board's servers would vest in my child upon creation, I agree to assign those rights to the Board.

Parent/Guardian's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Student**

I have read and agree to abide by the Student Network and Internet Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy and Guidelines is inappropriate and may constitute a criminal offense. As a user of the Board's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Student's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Teachers and building principals are responsible for determining what is unauthorized or inappropriate use. The principal may deny, revoke or suspend access to the Network/Internet to individuals who violate the Board's Student Network and Internet Acceptable Use and Safety Policy and related Guidelines, and take such other disciplinary action as is appropriate pursuant to the**

