7540.04 - **STAFF 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 District Information & Technology Resources (as defined by Bylaw 0100) (collectively, "District Information & Technology Resources") to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for educational purposes only and utilizes apps and services (apps/services) (as defined by Bylaw 0100) to enhance the instruction delivered to its students and to facilitate the staff's work. 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 by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staff's use of District Information & Technology Resources and personal communication devices when they are connected to the District's Information & Technology Resources, including apps/services, regardless of whether such use takes place on or off school property (see Policy 7530.02).

Staff members 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 (e.g., making personal attacks and injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on a staff member's First Amendment rights. Because District 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.

Staff members 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).

Staff members are expected to use District Information & Technology Resources to promote educational excellence in our schools by providing students with the opportunity to develop resource-sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and apps/services will be guided by Board Policy 2520 - Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that brings incredible education and information resources to our students. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District Information & Technology Resources provide students and staff with the opportunity to communicate with people throughout the world. Access to such an incredible quantity and diversity of information and resources brings with it, however, certain unique challenges and responsibilities.

While the Board uses various technologies to limit the use of District Information & Technology Resources to only use/access apps/services and resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent users 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 all 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 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 Superintendent, the technology protection measures may also 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 staff members 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 staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be disciplined, up to and including termination.

The Superintendent or Director of Technology 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. The Superintendent or Director of Technology may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

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

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

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

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students or staff 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. Further, staff members shall monitor students' online activities while the students 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 disclosure of personally identifiable information about students online is prohibited.

All staff members who use District Information & Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines. See Form 7540.04 F1.

In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, staff members are required to comply with all District-established cybersecurity procedures.

Staff will be assigned a District-provided school e-mail address that they are required to use for all school-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the District.

With prior approval from the Superintendent or Director of Technology, staff may direct students who have been issued school-assigned e-mail accounts to use those accounts when signing-up/registering for access to various apps/services that the students will utilize for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District Information & Technology Resources - i.e., behavior comparable to that expected 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 rules for professional behavior and communication apply. The Board does not approve any use of District Information &

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

Staff members may only use District Information & Technology Resources to access or use social media if it is done for educational or business-related purposes.

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's personal communication device. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Use of Artificial Intelligence Tools

Staff are permitted to use Artificial Intelligence ("AI") tools to accomplish their job responsibilities so long as the use is ethical, responsible, and does not violate any provisions of this policy – e.g., it does not infringe on students' or staff members' privacy rights, violate their duty to maintain confidentiality related to PII, etc..

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. (See Policy 7540.09 - Artificial Intelligence ("AI"))

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 Director of Technology as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District Information & Technology Resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting PII about students is not permitted. Staff members who violate State and Federal confidentiality and/or privacy laws related to the disclosure of student or employee PII may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

Revised 1/06
Revised 11/16/09
Revised 8/20/12

Revised 11/17/14

Revised 5/20/19

© Neola 2024

7540.04 – STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
Staff Agreement & Signature Page

By signing below, I acknowledge that I have received, read, and understand Board Policy **7540.04 – Staff Technology Acceptable Use and Safety**, including all related administrative guidelines and procedures.

I agree to comply with the terms and conditions outlined in this policy, including but not limited to:

- Appropriate and lawful use of District Information & Technology Resources
- Adherence to cybersecurity procedures and data privacy requirements
- Protection of personally identifiable information (PII)
- Responsible and professional use of communication tools and social media
- Compliance with all expectations regarding Artificial Intelligence (AI) tools
- Understanding that use of District resources may be monitored and is not private

I understand that access to District Information & Technology Resources is a privilege, not a right, and that violations of this policy may result in disciplinary action, up to and including termination of employment, as well as possible civil and/or criminal liability.

Staff Member Name (Print): _____

Staff Member Signature: _____

Phone: _____

Date: _____

Position/Title: _____

School/Building: _____

This signed agreement will be maintained in accordance with District recordkeeping procedures.