SECOND READING BY BOARD

po7540.04

Vol. 35, No. 2 - Artificial Intelligence (AI) - July 2026 Revised STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

7540.04 - **STAFF 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 and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps 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 limited educational purpose.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related administrative guidelines Policy 7544 - Use of Social Media and AG 7544 - Use of Social Media, and any applicable employment contracts govern the staff's use of the District's computers, laptops, tablets, personal communication devices (as defined by Policy 7540.02- Digital Content and Accessibility ~~Web Content, Apps, and Services~~), when they are connected to the District computer network, Internet connection, and/or educational services/apps.

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 the use of the bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information 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).

Staff members are expected to utilize District technology and information resources to promote educational excellence in our schools by providing students with the opportunity to develop the 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 to enrich educational activities. The instructional use of the Internet and online educational services will be guided by the Board's Policy 2521 - Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that provides a valuable education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District technology and resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such a vast quantity of information and resources brings with it, however, certain unique challenges.

The Board may not be able to technologically limit access to services through its technology resources to only those 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.

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. 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 the District's technology resources if such disabling will cease to protect against access to materials that are prohibited under the Children’s Internet Protection Act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The Board utilizes software and/or hardware to monitor online activity of staff and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254 (h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

The Superintendent or designee may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether the 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 Designee may disable the technology protection measure to enable access for bona fide research or other lawful purposes for staff . ~~or students aged seventeen (17) or older.~~

Authorized and Appropriate Use of Artificial Intelligence (AI)

Staff are expected to use District-approved AI tools responsibly and ethically to support essential professional functions, including, but not limited to, instruction, providing student feedback, and improving workflow efficiency.

All use of AI technology by staff must adhere to the requirements and standards detailed in Policy 7540.08 – Artificial Intelligence (AI).

Use of AI to Generate any Synthetic Intimate Representation

Any staff member or student suspected of using AI or other technological means to create a synthetic intimate representation will be referred to law enforcement in addition to any disciplinary action imposed by administration. Synthetic Intimate Representation means a representation of a nude or partially nude person, or of a person engaged in sexual activity, or as otherwise prohibited by law that is generated using technological means that uses an identifiable person's face, likeness, or other distinguishing characteristic to depict an intimate representation of that person, regardless of whether the representation includes components that are artificial, legally generated, or generally accessible, and that

is so realistic that a reasonable person would believe it depicts conduct of the identifiable person.

AI Prohibited Data Input

Staff shall use AI tools responsibly, ethically, and in compliance with district technology, student records, and data privacy policies.

Staff must not enter student Personally Identifiable Information (PII), staff PII, or proprietary District data into any AI system or service unless it has been explicitly reviewed, approved, and contracted by the District.

Staff members are prohibited from using AI tools to bully, harass, threaten, impersonate, or create or distribute deceptive or harmful content, including deepfake or synthetic media that falsely depicts another person. AI may not be used in ways that violate student or employee privacy, compromise confidential information, engage in academic or professional misconduct, or otherwise disrupt the educational environment.

Any misuse of AI that violates Board policy, professional standards, or applicable law may result in disciplinary action, up to and including termination of employment.

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

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

B. the inherent danger of students disclosing personally identifiable information when using AI and when 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 regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate technology use and online safety and security as specified above, and staff members will monitor students' online activities 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.

The disclosure of personally identifiable information about students online is prohibited.

Building Principals are responsible for providing training so that staff users of District technology resources 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 the 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 chat rooms and cyberbullying awareness and response. All users of District technology resources are required to confirm their agreement to abide by the terms and conditions of this policy and its accompanying guidelines by signing the District technology use form. Pursuant to Policy 7540.06 - District-Issued Staff E-Mail Account, staff and Board members using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use of District-issued email accounts.

Off premises use of E-Rate supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

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

[X] With prior approval from the Superintendent, staff may direct students who have been issued school-assigned email accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District technology and information resources - i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of the technology and information resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines and Policy 7544 - Use of Social Media and its accompanying guideline.

~~[DRAFTING NOTE: Choose the option above if the District Administrator recommends and the Board adopts Policy 7544 .]~~

~~[DRAFTING NOTE: If the use of social media is authorized by Policy 7540 and Policy 7544 , choose the appropriate option to match that language]~~

~~[ ] Staff members may only use District technology resources to access or use social media if it is done for educational or business-related purposes.~~

~~[ ] Staff members' use of District technology resources to access or use social media is to be consistent with Policy 7544 and its accompanying guideline.~~

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 computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

General school rules for behavior and communication apply.

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 and information resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and designee as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District technology and information 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 personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential employee information may be disciplined.

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

Revised 9/27/17
Revised 11/18/20
Revised 9/24/24

© Neola 202 6 ~~4~~

Legal

P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246
20 U.S.C. 6777, 9134 (2003)
47 C.F.R. 54.500 - 54.523

118.07(7), Wis. Stats.