SECOND READING BY BOARD

po7540.03

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

ADOPTED May 25, 2016 · REVISED Aug 19, 2026

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 provides technology resources (as defined in Bylaw 0100 - Definitions) 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 - Personal Communication Devices).

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).

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 the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measures may not be disabled at any time that students may be using the 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 Board utilizes software and/or hardware to monitor online activity of students 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 as to minors.

At the discretion of the Board or the Superintendent, the technology protection measure may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measure may not be disabled at any time that students may be using the 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 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 measure. 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 measure.

The Superintendent or designee may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

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;

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 the District technology use form. This agreement remains active until the student leaves the District unless explicitly revoked by a parent.

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.

Students will be assigned a school email 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 email 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. 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.

~~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.~~

Appropriate Discussion Content When Using PCDs (Personal Communication Devices)

When using PCDs to communicate with Board members, staff and/or volunteers, students must use District-approved communication platforms.

~~The approved communication platform(s) is/are:~~

A. ~~District email/messaging;~~

B. ~~District-approved social media platform(s) - (see also Policy 7544 - Use of Social Media);~~

C. ~~District-approved communication apps.~~

~~The District-approved communication platform(s) shall be listed on the District's website.~~

When students communicate with staff, volunteers, or Board members using PCDs, discussions must be appropriate, professional, and related to legitimate school purposes. These communications shall occur only when absolutely necessary. Appropriate content includes:

A. Instructional communication (assignments, coursework, academic support);

B. School-related activities (clubs, athletics, events, field trips, rehearsals);

C. Scheduling or logistical information related to classes or school programs;

D. Pedagogical assistance related to school participation (clarifying expectations, reminders, or academic assistance); and

E. Safety or emergency communication when necessary.

Communications must remain professional in tone, limited to educational or school-related matters, and consistent with District policies regarding staff–student boundaries. Failure to follow these policy expectations may result in discipline up to and including termination, as well as referral to law enforcement if deemed appropriate. The level of discipline will depend on the severity of the violation. This policy applies to communication that occurs during or outside of school hours.

AI Prohibited Data Input ~~Expectations for Responsible Artificial Intelligence (AI) Use~~

~~Students are strictly prohibited from inputting Personally Identifiable Information (PII), confidential student or staff data, or any non-public school records into any AI tool or service that has not been explicitly approved and contracted with by the District.~~

~~Students are expected to adhere to principles of transparency, proper citation, and responsible use of AI in all academic and school-related activities. Students must disclose the use and extent of AI assistance on any submitted work as required by staff.~~

Students are prohibited from using technology and/or AI to bully, harass, threaten, impersonate, create, or distribute deceptive or harmful content, including deepfake or synthetic media that falsely depicts another person. AI may not be used for academic dishonesty, privacy violations, or any conduct that materially disrupts the educational environment. Violations of this policy will result in disciplinary action consistent with Policy 5500 - Student Codes of Conduct and other applicable Board policies.

Academic Honesty

The unauthorized use of Artificial Intelligence tools to generate or complete academic work shall constitute a violation of the District's policy on academic honesty. (See Policy 5505 - Academic Honesty)

~~All student use of AI technology must comply with the requirements and standards set forth in Policy 7540.08 – Artificial Intelligence (AI).~~

~~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.

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 students' use of District technology resources.

Revised 9/27/17

Revised 11/4/17
Revised 11/18/20

Revised 5/21/25

© Neola 2026

Legal
H.R. 4577, 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
18 U.S.C. 2256

18 U.S.C. 1460
18 U.S.C. 2246
47 C.F.R. 54.500
47 C.F.R. 54.501
47 C.F.R. 54.502
47 C.F.R. 54.503
47 C.F.R. 54.504
47 C.F.R. 54.505
47 C.F.R. 54.506
47 C.F.R. 54.507
47 C.F.R. 54.508
47 C.F.R. 54.509
47 C.F.R. 54.511
47 C.F.R. 54.513
47 C.F.R. 54.514
47 C.F.R. 54.515
47 C.F.R. 54.516
47 C.F.R. 54.517
47 C.F.R. 54.518
47 C.F.R. 54.519
47 C.F.R. 54.520
47 C.F.R. 54.522
47 C.F.R. 54.523
942.09, Wis. Stats.
118.07(7), Wis. Stats.