Book	Policy Manual
Section	For Board Review - Vol. 34, No. 1
Title	STAFF EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.04
Status	
Adopted	April 23, 2007
Last Revised	October 16, 2023

7540.04 - **STAFF EDUCATION 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 by Bylaw 0100 - Definitions) and Information Resources (as defined by Bylaw 0100 - Definitions) 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 Resources 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 - 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~~the District's Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology Resources 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 ~~t~~Technology Resources and ~~I~~information R~~r~~esources 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, the ~~e~~Education ~~t~~Technology provides 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 ~~e~~Education ~~t~~Technology 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 ~~e~~Education ~~t~~Technology 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 containing appropriate material if access to such sites has been inappropriately 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 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.

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 online; and,

C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students or staff online;

D. unauthorized disclosure, use, and dissemination of personal 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 the Principal's 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 Internet. All Internet users are required to confirm their agreement to abide by the terms and conditions of this policy and its accompanying guidelines during the Employee Handbook receipt and acceptance process. 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.

~~**[Drafting Note: If the District participates in the Federal Universal Service E-Rate Program for Schools, the Federal Communications Commission (FCC) requires the following language be included in your acceptable use policy.]**~~

~~-~~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, and vendors or individuals seeking to do business with the District. Staff shall not use their school-assigned email account for non-school-related electronic communications or to signup/or register for any non-school-related mobile applications/apps.

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 on the District's computers/network and the Internet just as they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines and Policy 7544 and its accompanying guideline.

Staff members may only use District T~~t~~echnology R~~r~~esources 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 computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Users who disregard this policy and its accompanying guidelines may have their use privileges restricted or revoked, and disciplinary action taken against them. Users granted access to the Internet through the District's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and the Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to the use of the Network and the Internet for instructional purposes.

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 - Student Records. 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 9/19/11
Revised 3/18/13
Revised 3/14/16
Revised 8/17/20
T.C. 10/16/23

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

20 U.S.C. 9134 (2003)

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