

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

Advances in telecommunications and other related technologies have fundamentally altered the ways in which information is accessed, communicated, and transferred in society. Such changes are driving the need for educators to adapt their means and methods of instruction, and the way they approach student learning, to harness and utilize the vast, diverse, and unique resources available on the Internet. The School Board is pleased to provide Internet service to its staff. The District's Internet system has a limited educational purpose. The District's Internet system has not been established as a public access service or a public forum. The Board has the right to place restrictions on its use to assure that use of the District's computers, network and Internet services ("Network") is in accord with its limited educational purpose. Staff use of the District's Network will be governed by this policy and the related administrative guidelines. Users should have no expectation of privacy in the content of any files or records of their online activity while on the Network.

The Board encourages staff to utilize the Internet 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 will be guided by the Board's policy on instructional materials.

Through the Internet, students and staff can access up-to-date, highly relevant information that will enhance their learning and the education process. Further, the Internet provides students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges.

First, and foremost, the Board may not be able to technologically limit access to services through the Board's Internet connection 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, will open classrooms and students to electronic information resources which have not been screened by educators for use by students of various ages.

The Board has implemented technology protection measures which block/filter Internet access to visual displays that are obscene, any pornography or harmful to minors. The Board 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 Superintendent or the Director of Technology 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;
- C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by students or staff online; and
- 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.

The Building principal is responsible for providing training so that Internet users under his/her 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 sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Staff members are responsible for good behavior on Board'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.

Use of Social Media

The School Board respects the rights of employees to use social networking sites as a medium of self-expression during non-work time. Employees are not permitted to use the social networking sites for personal use during work time.

Employee Use of Social Networking Sites for Educational and Professional Purposes: The School Board understands that technology is constantly changing and encourages employees to use technology to assist with student learning. Employees may use social networking sites for educational purposes under the following

- A. The Superintendent or designee must approve all social network sites and groups prior to use by the employee with students.
- B. The building administrator must be a part of any school or non-social network site and group between any employee and student.
- C. Employees must document and retain all electronic communication between themselves and students. (Policy 4.19 Professional Expectations for District Employees)

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the Board'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 Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of the Network.

Social Media Use -An employee's personal or private use of social media, such as Facebook, Twitter, MySpace, blogs, etc., 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 private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

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.

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 76 F.R. 56295, 56303