

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 our 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 Board of Education is pleased to provide network and Internet service to its staff. The Board encourages staff to utilize the District network and Internet in order to promote educational excellence in our schools by providing them with the opportunity to develop the resource sharing, innovation, and communication skills and tools which will be essential to life and work in the 21st century. The Board expects the staff to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources. The instructional use of the Internet will be guided by the Board's policy on Instructional Materials (Policy 2521).

The Board has implemented technology protection measures which block/filter Internet access to visual displays that are obscene, child pornography or harmful to minors. The Board utilizes software and/or hardware to monitor online activity of staff members to restrict access to pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The Superintendent or Director of Technology may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

The Superintendent is directed to prepare guidelines which address staff members' safety and security while using e-mail, social media, and other forms of direct electronic communication. These guidelines will prohibit disclosure of personal identification information, unauthorized access (e.g., "hacking"), and other unlawful online activities. Staff members are reminded that personally identifiable student information is confidential and may not be disclosed without prior written parental permission.

Director of Technology and Technology staff are responsible for providing training so that district network / Internet users are knowledgeable about this policy and its accompanying guidelines.

Training shall include:

- A. Safety and security while using e-mail, chat rooms, social media, and other forms of electronic communications;
- B. The inherent dangers of 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; **and**
- D. Unauthorized disclosure, use, and dissemination of personal information regarding minors.**

Social media shall be defined as internet-based applications (such as Facebook, Twitter, Blogger, etc.) that incorporate interactive communication between users. The District authorizes the instructional staff to utilize social media tools using the District’s network provided such access has an educational purpose for which the instructional staff member has ~~the prior approval~~ **to use the specific social media application.** ~~of the building principal, the Director of Technology, and Assistant Superintendent of Curriculum and Instruction.~~ (Specific guidelines for the use of electronic communication and the use and approval of social media for school related purposes are outlined in AG 7540.04)

The Board expects that staff members will provide guidance and instruction ~~to students in the appropriate use of the District network and Internet to students in the appropriate use of the Internet~~ **for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members may monitor the online activities of the students under their supervision 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.

All network / 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 appropriate behavior on the District network and 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 district rules for behavior and communication apply. The Board

**BOARD OF EDUCATION
GENEVA COMMUNITY UNIT
SCHOOL DISTRICT #304**

PROPERTY
7540.04/page 3 of 3

does not sanction any use of the network / Internet 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 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 the use of the network and the Internet for instructional, professional, ethical, legal, and operational purposes.

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

Adopted 12/11/06
Revised 12/28/2010
Revised 7/18/2011
Revised 7/18/2012 Janowiak
To Policy Committee 8/27/2012