Code No. 605.6

STAFF USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS

The Internet and electronic communications (e-mail, chat rooms and other forms of electronic communication) have vast potential to support curriculum and learning. The Board of Education believes they should be used in schools as a learning resource to educate and to inform.

The Board of Education supports the use of the Internet and electronic communications by staff to improve teaching and learning through interpersonal communication, access to information, research, training and collaboration and dissemination of successful educational practices, methods and materials.

The Board believes the educational opportunities inherent in these tools far outweigh the possibility that users may procure material not consistent with the education goals of the district. However, the Internet and electronic communications are fluid environments in which users may access materials and information from many sources. Staff members shall take responsibility for their own use of district computers and computer systems to avoid contact with material or information that violates this policy.

To protect students from material and information that is obscene, child pornography or otherwise harmful to minors, software that blocks or filters such material and information is used by the District. Blocking or filtering software may be disabled by the District Technology Coordinator, or designee, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

District computers and computer systems are owned by the district and are intended for educational purposes and district business. Staff members shall have no expectation of privacy when using the Internet or electronic communications. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials and information, All material and information accessed/received through district computers and computer systems shall remain the property of the school district. Staff members shall use district computers and computer systems in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of district computers and computers systems cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to the following.

No staff member shall access, create, transmit, retransmit or forward material or information:

that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons;

that is not related to district education objectives;

that contains pornographic, obscene or other sexually oriented materials either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion;

that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons;

for personal profit, financial gain, advertising, commercial transaction or political purposes;

that plagiarizes the work of another;

that uses inappropriate or profane language;

that is knowingly false or could be construed as intending to purposely damage another person's reputation;

in violation of any federal or state law, including but not limited to copyrighted material and material protected by trade secret;

that contains information protected by confidentiality laws;

using another individual's Internet or electronic communications account without written permission from that individual; or

that impersonates another or transmits through an anonymous remailer.

Security on district computer systems is a high priority. Staff members who identify a security problem while using the Internet or electronic communications or who inadvertently access inappropriate content or sites must immediately notify the District Technology Coordinator. Staff members should not demonstrate the problem to other users.

Staff members shall not:

use another person's password or any other identifier;

gain or attempt to gain unauthorized access to district computers or computers systems;

read, alter, delete or copy, or attempt to do so, electronic communications of other system users; or

bypass or attempt to bypass or otherwise defeat system security setting.

Any staff member identified as a security risk, may be denied access to the Internet and electronic communications.

Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians or district employees that is protected by confidentiality laws. If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a "need to know" are allowed access to the material.

Vandalism will result in cancellation of privileges and may result in school disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt operation of any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Staff members are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner.

Use of the Internet and electronic communications demands personal responsibility and understanding of the acceptable and unacceptable uses of such tools. Staff member use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy will result in the loss of the privilege to use these tools and may result in school disciplinary action up to and including termination and/or legal action. The school district may deny, revoke or suspend access to district technology or close accounts at any time. Staff members shall be required to sign the district's Acceptable Use Agreement upon initial employment before Internet or electronic communications accounts shall be issued or access shall be allowed.

The school district makes no warranties of any kind, whether expressed or implied, related to the use of district computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the district of the content, nor does the district make any guarantee as to the accuracy or quality of information received. The School District shall not be responsible for any damages, losses or costs a staff member suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the staff member's own risk.

Legal References:
47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 U.S.C. 231 (Child Online Protection Act of 1998)
20 U.S.C. 6801 et seq. (Elementary and Secondary Education Act)
Iowa code 279.8 (2007)

Approved 1/27/10
Grinnell-Newburg School District, Grinnell, IA