STAFF USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS

BLOCKING OR FILTERING OBSCENE, PORNOGRAPHIC, AND HARMFUL INFORMATION

To protect students from material and information that is obscene, child pornography or otherwise harmful to minors, as defined by the Board, software that blocks or filters such material and information has been installed on all district computers having Internet or electronic communications access. Blocking or filtering software may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

NO EXPECTATION OF PRIVACY

District computers and computer systems are owned by the district and are intended for educational purposes and district business at all times. 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.

BLOCKING OR FILTERING OBSCENE, PORNOGRAPHIC, AND HARMFUL INFORMATION

To protect students from material and information that is obscene, child pornography or otherwise harmful to minors, as defined by the Board, hardware that blocks or filters such material and information has been installed on all district computers having Internet or electronic communications access. Blocking or filtering hardware may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

UNAUTHORIZED AND UNACCEPTABLE USES

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 computer 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:

1. 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

2. that is not related to district education objectives

3. that contains pornographic, obscene or other sexually oriented materials,

4. that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, sex, religion, national origin, age, marital status disability or handicap.

5. for personal profit, financial gain, advertising, or commercial transaction

6. that plagiarizes the work of another

7. that uses inappropriate or profane language likely to be offensive to others in the school community

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

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

10. that contains personal information about themselves or others, including information protected by confidentiality laws

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

12. that impersonates another or transmits through an anonymous remailer

SECURITY

Security on district computer systems is a high priority. Staff members who identify a security problem while using the Internet or electronic communications must immediately notify a system administrator. Staff members should not demonstrate

the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Staff members shall not:

1. use another person's password or any other identifier

2. gain or attempt to gain unauthorized access to district computers or computer systems

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

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

CONFIDENTIALITY

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. Staff members shall handle all employee, student and district records in accordance with policies GBJ (Personnel Records and Files), JRA/JRC (Student Records/Release of Information on Students) and EGAEA (Public Electronic Mail Records).

VANDALISM

Vandalism directed at the computer communications system 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.

UNAUTHORIZED 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.

STAFF MEMBER USE IS A PRIVILEGE

Use of the Internet and electronic communications demands personal responsibility and an 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 shall result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in school disciplinary action 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 before Internet or electronic communications accounts shall be issued or access shall be allowed.

SCHOOL DISTRICT MAKES NO WARRANTIES

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.

ADOPTED: September 10, 2002

LEGAL REFS.: 47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 U.S.C. 231 et seq. (Child Online Protection Act of 2000)
20 U.S.C. 6801 et seq. (Elementary and Secondary Education Act)