Staff Use of District Technology

In accordance with the Board's policy on Staff Use of District Technology, staff members shall not:

1. Access, transmit or retransmit any material in violation of any U.S. or state law, including but not limited to copyrighted material and material protected by trade secret.

2. Access, 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 and student records in accordance with policies GBJ (Personnel Records and Files), JRA/JRC (Student Records/Release of Information on Students) and EGAEA (Electronic Mail).

3. Access, transmit or retransmit material which is threatening, promotes violence or advocates destruction of property including, but not limited to, information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices or the like.

4. Communicate with a student or students through social media or social networking unless for educational purposes, and it is approved by district supervisory personnel, parents are notified, and consent is given to do so.

5. Access, transmit or retransmit any information containing pornographic, obscene or other sexually oriented material.

6. Access, transmit or retransmit material which advocates or promotes violence or hatred against particular individuals or groups of individuals or advocates or promotes the superiority of one group over another (for example: racial, ethnic, religious, etc.)

7. Use inappropriate or profane language or access, transmit or retransmit material likely to be offensive to others in the school community, including sexually harassing material.

8. Use or possess unauthorized or bootleg software (bootleg software means any software which has been downloaded or is otherwise in the user's possession without the appropriate registration of the software including the payment of any fees owing to the owner of the software).

9. Impersonate another user or transmit or retransmit material anonymously.

10. Use another district employee's network account or modify files, passwords or data belonging to other users in the district.

11. Access fee services via district technology without specific permission from the system administrator.

12. Use district technology for personal profit or for non-school related purposes.

13. Destroy, modify or abuse district owned technology or disrupt the operation of any network within the school district or any network connected to the Internet, including the use, attempted use or possession of computer viruses.

14. Fail to report any violation of the provisions contained herein to his or her supervisor.

Approved: 11/11/99

Revised: 02/11/16