

STAFF TECHNOLOGY USE/SOCIAL NETWORKING REGULATION

General

The following rules and regulations govern the use of the school district's computer network system, employee access to the Internet, and management of computerized records:

- Employees will be issued a school district e-mail account. Passwords must be changed periodically.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- Employees are expected to review their e-mail regularly, and shall reply promptly to inquiries with information that the employee can reasonably be expected to provide.
- Communications with parents and/or students must be made on a school district computer, unless in the case of an emergency, and should be saved and the school district will archive the e-mail records according to procedures developed by the technology director.
- Employees may access the Internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use, including access to social networking sites when it disrupts the education and supervision of students.
- Use of the school district computers and school e-mail address is a public record. Employees cannot have an expectation of privacy in the use of the school district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline, up to and including discharge.
- Use of the school district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Off-site access to the school district computer network will be determined by the superintendent in conjunction with appropriate personnel.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the school district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of school district computer use guidelines may be denied access to the school district's network.

Prohibited Activity and Uses

The following is a list of prohibited activity for all employees concerning use of the school district's computer network. Any violation of these prohibitions may result in discipline, up to

and including discharge, or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising, or personal gain.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the school district computer network. See Policy 605.7, Use of Information Resources for more information.
- Using the network to access inappropriate web sites, e.g. pornographic, on the school district network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, and abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy school district equipment or materials, data of another user of the school district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages during a time that disrupts the education or supervision of students. (The user further understands that most all information on the school district's computer system is considered a public record. Therefore, users of the school district's computer network must not expect, nor does the school district guarantee, privacy for e-mail or use of the school district's computer network including web sites visited.)
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the school district's computers and/or network without the permission of the superintendent.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Other Technology Issues

Employees should not release their cell phone number, personal e-mail address, etc. to students or their parents, unless in the case of an emergency. Employees, who are coaches or sponsors of activities, may create a text list of students and parents in order to communicate more effectively as long as the texts go to all students and the principal is included in the text address list.

Approved: July 16, 2012

Reviewed:

Revised: August 20, 2012