BOARD POLICY 401.060

STAFF TECHNOLOGY USE 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 throughout the day, 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 archived. The e-mail should also be cc'd to the building administrator.
- 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.
- 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.
- 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.
- 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 district Technology Director.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Social Networking or Other External Web Sites

For purposes of this policy any web site, other than the school district web site or school-school district sanctioned web sites, are considered external web sites. Employees shall not post confidential or proprietary information, including photographic images, about the school district, its employees, students, agents or others on any external web site without consent of the superintendent. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the school district when on external web sites. Employees shall not use the school district logos, images, iconography, etc. on external web sites. Employees shall not use school district time or property on external sites that are not in direct-relation to the employee's job. Employees, students and volunteers need to realize that the Internet is not a closed system and anything posted on an external site may be viewed by others, all over the world. Employees, students and volunteers who don't want school administrators to know their personal information, should refrain from exposing it on the Internet. Employees, who would like to start a social media site for school district sanctioned activities, should contact their building administrator.

Other Technology Issues

Employees with personal cell phones should not be using the phones for school district business. Employees should contact students and their parents through the school district computer or phone unless in the case of an emergency or with prior consent of the principal. Employees should not release their cell phone number, personal e-mail address, etc. to students or their parents. 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.