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 should review their e-mail regularly (daily checks if possible), and shall reply in a timely manner to inquiries with information that the employee can reasonably be expected to provide.
- Communications with parents and/or students may be made on a school district computer.
- Employees may access the Internet for education-related and/or work-related activities.
- Employees shall keep to a minimum 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.
- 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 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 receive, transmit or make available to others obscene, offensive, or sexually explicit material.

STAFF TECHNOLOGY USE REGULATION

- Postings that contain content that disrupts the educational program and damages the relationships of trust necessary between students, staff and parents are strictly prohibited. Examples include but are not limited to content that:
    - o Is sexually provocative or flirtatious in nature;
    - o Exhibits or advocates for use of drugs and alcohol;
    - o Would be defined by a reasonable person as obscene, racist, or sexist;
    - o Promotes illicit, illegal or unethical activity;
    - o Violates the district's affirmative action and/or bullying and harassment policies.
- Postings that communicate confidential information to persons not authorized to receive that information are prohibited.
- Postings that cause significant interference with the education program via any electronic means are prohibited.
- 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.
- 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.
- Using the network for sending and/or receiving personal messages shall be kept to a minimum.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software on the school district's computers and/or network without the permission of the Director of Technology.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Approved: December 10, 2012

Reviewed: December 8, 2014

Revised: