Policy Title: Staff Technology Use/Social Networking Regulation
General

Code No. 402.6-R

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.
- Employees may access the Internet for education-related and/or work-related activities.
- 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.
- All communications are expected to abide by the generally accepted rules of 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.
- Report, as required by law, any information found on a social networking site that falls under the mandatory reporting guidelines.
- All passwords are to be kept private and not shared with anyone else. Failure to keep your password private may lead to disciplinary action.
- Users will lock and or log out of district computers when unsupervised. Failure to lock or log out when a computer is not in use may lead to disciplinary action. Computer policies will be used to automatically log out of computers when left unattended for a period of time.
- Users will be locked out of their computer system after 3 failed login attempts.

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 602.11, Use of Information Resources for more information.

- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material
- Submitting or posting confidential or protected information about the District, its students, alumni or employees. You should assume that most information about a student is protected from disclosure by both federal law (the Family Educational Rights and Privacy Act (FERPA) and state law (Iowa Code Section 22.7(1)). Disclosure of confidential or protected information may result in liability for invasion of privacy or defamation and result in disciplinary action up to, and including, discharge from employment
- All student images fall under both federal law (the Family Educational Rights and Privacy Act (FERPA) and state law (Iowa Code Section 22.7(1)). Student release forms are signed at the start of the school year and are stored in the online student records system. No student images should be posted to any social media presence without first ensuring permission for use has been granted. This includes group photos. Please see the District Permissions form for details about using photos from public events.
- 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 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.
- Using the network in a fashion inconsistent with generally accepted network etiquette.

Other Technology Issues

If a personal device is being used for school district business, employees must conduct themselves in a professional manner.

Adopted: May 1, 2017

Reviewed:

Amended: December 2, 2019