Regulation 713-R(1): Responsible Technology Use & Social Networking - Administrative Regs.

Status: ADOPTED

Original Adopted Date: 12/01/1996 **| Last Revised Date:** 03/25/2024 **| Last Reviewed Date:** 03/25/2024

General
The following rules and regulations govern the use of the school district's network systems, employee access to the internet, and management of digital records:

- Employees will be issued a school district e-mail account. Passwords must be changed periodically, and all employee email accounts must be protected by multi-factor authentication.
- 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 district-approved communication platforms , unless in the case of an emergency.
- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using technology resources for personal use, including access to social networking sites.
- Use of the school district technology and school e-mail address is a public record. Employees cannot have an expectation of privacy in the use of the school district's network and technology.
- Use of technology 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 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 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 technology use guidelines may be denied access to the school district's network.
- Employees are representatives of the district at all times and must model appropriate character, both on and off the worksite. This applies to material posted with personal devices and on personal websites and/or social media accounts. Posted messages or pictures which diminish the professionalism or discredit the capacity to maintain respect of students and parents may result in disciplinary action up to and including termination if the content posted is found to be disruptive to the educational environment and adversely impacts the employee's ability to effectively serve as a role model or perform his/her job duties for the district. The type of material that would affect an employee's ability to serve as an appropriate role model includes, but is not limited to, text or depictions involving hate speech, nudity, obscenity, vulgarity or sexually explicit content.
- Employee communications with students should be limited as appropriate. If there is any uncertainty, employees should consult their building administrator.

Prohibited Activity and Uses

The following is a list of prohibited activities for all employees concerning use of the school district's 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 network. See *Policy 605.07, Use of Information Resources* for more information.
- Violating the terms of service of commercial streaming platforms by viewing or sharing content intended for private, in-home use.
- 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 virus or other malware 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 technology on the school district's technology 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.

Other Technology Issues

Employees and volunteers, including coaches and sponsors of activities, should contact students and their parents through district-approved communication platforms or the district phone system unless in the case of an emergency or with prior consent of the Director of Communications. Information on district-approved communication platforms is available from the Director of Communications, Directory of Technology, or their designees.
