8630-R

COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION

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

I. Administration

- The Superintendent of Schools shall designate the Assistant Superintendent for Technology & Information Management to oversee the district's computer network.
- The Assistant Superintendent for Technology & Information Management shall monitor and examine all network activities, as appropriate, to ensure proper use of the system. The Assistant Superintendent for Technology & Information Management shall work with the [Network Administrator to maintain an updated inventory of all computer hardware and software resources.
- The Assistant Superintendent for Technology & Information Management shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery and notification plan and will comply with the requirements for records retention in compliance with the district’s policy on School District Records (1120), taking into account the use of onsite storage or storage in the cloud.
- The Assistant Superintendent for Technology & Information Management hall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The Assistant Superintendent for Technology & Information Management shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations (including policy 4526, Computer Use in Instruction) governing use of the district's network.
- The Assistant Superintendent for Technology & Information Management shall take reasonable steps to protect the network from viruses, other software, and network security risks that would compromise the network or district information.
- All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the Assistant Superintendent for Technology & Information Management, will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

II. Internet Access

Student Internet access is addressed in policy and regulation 4526, Computer Use in Instruction. District employees and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's computer network.
- Employees are expected to review their e-mail daily.
- Communications with parents and/or students should be saved as appropriate and the district will archive the e-mail records according to procedures developed by the Assistant Superintendent for Technology & Information Management.
- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use.
- Employees are advised that they must not have an expectation of privacy in the use of the district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to all staff and third party users of the district's computer system:

- Access to the district's computer network is provided solely for educational and/or research purposes and management of district operations consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically and must be of sufficient complexity as determined by the district.
- Only those network users with permission from the Assistant Superintendent for Technology & Information Management may access the district's system from offsite (e.g., from home).
- All network users are expected to take reasonable precautions to secure district information stored on devices they use, including maintaining responsible custody over computer resources, ensuring no unauthorized use of district devices, and exercising prudent judgment when browsing the internet and opening email.

- All network users are responsible to have their own device(s) and external flash drives / external hard drives or other media inspected and approved by MIS before they connect to the district's infrastructure.
- 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 district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity for all staff and third party users concerning the use of the district's computer network. Any violation of these prohibitions may result in discipline or other appropriate penalties, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting, or making available any copyrighted software on the 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 other messages that are racist, sexist, 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 district equipment or materials, data of another user of the 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, malware on the network, and not reporting security risks as appropriate.
- 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.
- Intentionally disrupting network traffic or crashing the network and connected systems.

- Installing personal software, using personal disks, or downloading files on the district's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for fraudulent purposes or financial gain.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while your access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Exhibiting careless behavior with regard to information security (e.g., sharing or displaying passwords, leaving computer equipment unsecured or unattended, etc.).
- Attempting to circumvent district filtering or security policies.

V. No Privacy Guarantee

Users of the district's computer network should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

VI. Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secrets. Users must respect all intellectual and property rights and laws.

VII. District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the user's own negligence or any other errors or omissions. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

The district will take reasonable steps to protect the information on the network and provide a secure network for data storage and use, including ensuring that contracts with vendors address data security issues and that district officials provide appropriate oversight. Disposal of district computer resources shall ensure the complete removal of district information, or the secure destruction of the resource. Even though the district may use technical and/or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: 06-23-20

Amended: 12-09-25