COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION 8630-R.1

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

I. ADMINISTRATION

- The Superintendent of Schools shall designate the Director of Information Services to oversee the district's computer network.
- The Director of Information Services shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Director of Information Services shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery plan and will comply with the requirements for records retention in compliance with the district's policy on school district records.
- The Director of Information Services shall 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 Director of Information Services shall take reasonable steps to protect the network from viruses or other software that would compromise the network.
- All employee, student opt out, and third party user agreements to abide by district policy and regulations shall be kept on file in the Information Services office. Students may be granted an account for up to one academic year at a time.
- Consistent with applicable internal controls, the Superintendent, in conjunction with the Assistant Superintendent of Administration and the Director of Information Services, will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

II. INTERNET ACCESS

District employees, students and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's computer network. Johnson City School District e-mail accounts are to be used for district business. Limited personal use is considered acceptable.
- Employees are expected to review their e-mail daily.

II. INTERNET ACCESS (Cont'd.)

- Users may access the Internet for education-related and/or work-related activities. Limited personal use is acceptable.
- Users 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. FINANCIAL SOFTWARE SECURITY

- Users may have access to financial software for work-related activity. This access is a privilege, not a right. This privilege can be revoked at any time.
- Access to financial software may be obtained by requesting the appropriate access via the BOCES help desk. These requests will be reviewed and approved or denied by the Assistant Superintendent for Administration.

IV. ACCEPTABLE USE AND CONDUCT

The following regulations apply to all staff, students 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. Limited personal use is acceptable.
- 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. Non-students will be required to periodically change this password, as per password guidelines on Non-Student Request for Computer Network and Internet Access (8630-E.2).
- 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.

V. PROHIBITED ACTIVITY AND USES

The following is a list of prohibited activity for all staff, students and third party users concerning use of the district's computer network. Any violation of these prohibitions may result in discipline or other appropriate penalty, 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 material including, but not limited to software, music and video 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 others 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 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.
- Using third party websites and/or proxies to circumvent district filters or firewalls.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks 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.

V. PROHIBITED ACTIVITY AND USES (Cont'd.)

- 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.)

VI. 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.

VII. 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 secret. Users must respect all intellectual and property rights and laws.

VIII. 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.

VIII. DISTRICT RESPONSIBILITIES (Cont'd.)

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, misdeliveries, or service interruptions caused by its 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.

Further, even though the district may use technical 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.