COMPUTER USE IN INSTRUCTION REGULATION

The following rules and regulations govern the use of the district's computer network system and access to the Internet.

I. Administration

- The Superintendent of Schools shall designate a computer network coordinator to oversee the district's computer network.
- The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The computer network coordinator 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 computer network coordinator 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 governing use of the district's network.
- The computer network coordinator shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- All student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.

II. Internet Access

- Students will be provided supervised Internet access for instructional purposes only during the school day. Acceptable activities include classroom work and high-quality research.
- Students will be provided with individual access accounts.
- Students may ***not*** browse the World Wide Web and are only to use the internet at appropriate sites as designated by their teacher and/or other supervisory staff.
- Students ***are not*** to participate in chat rooms or any other social network sites.

- To the extent possible, staff members will supervise and monitor the online activities of students.

III. Acceptable Use and Conduct

- The District will conduct periodic reviews of all accounts to determine adherence to the goals of research and education.
- Use of the district's computer network is a privilege, not a right. Students using school computer networks are as responsible for good behavior as they are in the classroom or other school property. Inappropriate use may result in the suspension or revocation of that privilege
- 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.
- Only those network users with written permission from the principal or computer network coordinator may access the district's system from off-site (e.g., from home).
- 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 or sexual language or images, vulgarities and swear words are all inappropriate.
- Attempts to login to the Internet or network as a "system administrator" will result in cancellation of user privileges.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or computer network coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- 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.
- Students are as responsible for good behavior on school computer networks as they are in a classroom, or all other school property. General school rules for behavior and communication apply, as outlined in the District's Code of Conduct.

- The right to network services is given to students who agree to act in a considerate and responsible manner, and who provide parental permission to use the same. Access is a privilege (which entails responsibilities) not a right!
- Users have the full responsibility for the use of account, and, under no conditions, should users share their accounts or passwords with any other person.
- Staff and employees may use the computer network to send or receive communications from parents of students in relation to educational issues regarding the child of that/those parents.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Staff and employees may use the computer network to send or receive communications from parents of students in relation to educational issues regarding the child of that/those parents."
- 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 others messages that are racist, sexist, abusive, or harassing to others.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Vandalism will result in cancellation of system privileges as well as possible prosecution.
- 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.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- 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 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 commercial or financial gain or fraud.
- 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 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.
- Use of network for conduction personal business.
- Using the Network for product advertisement or political lobbying.

- No personal software or disks may be loaded onto the District's computers and/or network without permission of designated District personnel and a virus check.
- Any use which violates the District's Code of Conduct, New York State, Local or Federal Law. This includes, but is not limited to: copyrighted materials; threatening or obscene material; expressions of bigotry, racism, or hate; or material protected by trade secret.

V. No Privacy Guarantee

Students, faculty, staff, district employees, and/or any other person(s) using the district computer network shall not expect, nor does the district provide any exception or guarantee of privacy for electronic mail (e-mail) or any use of the district's computer network in any manner or for any purpose whatsoever. The district reserves its full and unconditional right to access and view any material transmitted, received or stored on district equipment and/or any material used for any purpose whatsoever in connection with the district's computer network.

Messages relating to or in support of illegal activities will be reported to school officials, parents, and where appropriate, to other proper authorities.

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.

In addition, illegal activities and/or improper, unprofessional, and/or personal uses unrelated to educational purposes of the district are strictly prohibited. Any illegal, and/or improper, unprofessional, and/or personal uses unrelated to education purposes of the district and/or the 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.

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 that is used and provided.

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 the errors or omissions of any user. 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.

VIII. Training

The Superintendent or his/her designee shall provide training and or notification to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.

The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.

First Reading: October 8, 2013
Adoption date: November 12, 2013
Revised First Reading: October 6, 2016
Adoption date: November 7, 2016
Revised First Reading: January 9, 2019
Adoption date: February 12, 2019