

## 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 and online resources.

### I. Administration

- The Superintendent of Schools shall designate a Director of Information Technology Services to oversee the district's computer network.
- The Department of Information Technology Services shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Department of Information Technology 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 Department of Information Technology in conjunction with the Department of Professional Development Services 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 Director of Information Technology Services shall ensure that all computer media, such as, but not limited to, disks, software and thumb drives (USB sticks) loaded onto the computer network have been scanned for computer viruses.
- The Director of Information Technology Services will review staff requests to use 'cloud-based' educational software/applications to ensure that personally identifiable information (PII) is protected in accordance with district standards prior to student use.
- 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 Internet access on site during class time, during the school day, before and after school hours for use as an instructional resource.
- Students will be provided with individual access accounts.
- Students may have Internet access for a range of educational purposes.
- Student Internet access may be restricted depending on the grade level.
- In order to access the Internet students must use the district's network while on school district property.
- All users will be prohibited from accessing social networking sites; playing online games; purchasing or selling anything online (unless authorized for district purposes); personal email services; and watching videos online (unless authorized for a school purpose).
- Students are **not** to participate in chat rooms unless under the supervision of a teacher or administrator.

- Students may **not** construct their own web pages using district computer resources unless under the supervision of a teacher or administrator.
- Students of specific grades will have individual e-mail addresses.

A staff member will be required to monitor all teachers & building administrators of these activities.

### III. Acceptable Use and Conduct

- Access to the district's computer network is provided for educational purposes and research 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.
- Only those network users who have properly registered their device with the Director of Information Technology Services, or who have been issued a district-owned device, may access the district's system from offsite (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.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator, or Director of Information Technology Services. 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.
- 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.

### IV. Prohibited Activity and Uses

The following is a list of prohibited activities concerning the use of the district's computer network. Violation of any 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.
- 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.
- 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.

#### V. No Privacy Guarantee

Students using 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.

#### 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 are strictly prohibited. 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 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, mis-deliveries, 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.

Adoption date: 06-23-20