( ) Required
(X) Local
(X) Notice

STAFF COMPUTER USE IN INSTRUCTION POLICY

The Floral Park-Bellerose Union Free School District Board is committed to optimizing student learning and teaching. The Board considers staff access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in District classrooms for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

Because the Internet is an unregulated, worldwide vehicle for communication, information available to staff and students is impossible to control fully. Therefore, the Board adopts this policy governing the use of electronic resources and the Internet in order to provide guidance to individuals and groups obtaining access to these resources on school department-owned equipment or through affiliated organizations.

All users of the District's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The District reserves the right to control access to the Internet for all users of its computers and network. The District may either allow or prohibit certain kinds of online activity, or access to specific websites.

In addition to activity on the District-owned technology network, the rules, guidelines, terms and conditions included in this regulation shall also apply to activity on Internet-based services and sites either subscribed to or endorsed by the District for staff use. These include, but are not limited to:

a. Learning management systems,
b. Online file storage/management systems,
c. Online document creation/management systems,
d. Online instructional sites,
e. Online video, audio, social media sites

Regulations and handbooks, to be developed by the Superintendent, in consultation with Director of Curriculum and Instructional Technology, District Network Administrator, Principals, Assistant Principals and the Technology Committee, will provide specific guidance on this, as well as rules governing the use and security of the District's computer network. All users of the District's computer network and equipment shall comply with this policy and regulation. Failure to comply may result in disciplinary action, if applicable, suspension and/or revocation of computer access privileges or other appropriate remedial action.

The Superintendent shall be responsible for designating a District Network Administrator to oversee the use of District computer resources. The District Network Administrator will prepare in service programs for the training and development of District staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Director of Curriculum and Instructional Technology and/or the District Network Administrator. The Director of Curriculum and Instructional Technology and/or the District Network Administrator will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

The Superintendent, working in conjunction with the designated purchasing agent for the District, the computer network coordinator and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout District schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or District needs.

Cross-ref: 5330, Code of Conduct

STAFF COMPUTER USE IN INSTRUCTION REGULATION

I. Administration

- The Superintendent of Schools shall designate a District Network Administrator 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. This may include real-time monitoring of Internet access and/or maintaining a log of Internet activity, or attempted activity, for later review.
- The District Network Administrator 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 District Network Administrator shall provide staff 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 District Network Administrator shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- The District Network Administrator 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 staff members agree to abide by District policy and regulations.

II. Internet Access

- Staff will be provided with Internet access on school grounds.
- Staff will be provided with individual access accounts.
- Staff may have Internet access for educational purposes only.
- In order to access the Internet students must use the District's network.
- Staff will be prohibited from: accessing social networking sites; playing online games; purchasing or selling anything online; personal email services; and watching videos online (unless authorized for a school purpose).
- Staff ***are not*** to participate in chat rooms, unless authorized for a school purpose including but not limited to student personal social media accounts.
- Staff ***may not*** construct their own web pages using district computer resources (unless authorized for a school purpose).
- Staff may have individual e-mail addresses. Email is to be used for school purposes only.

While the District has programs in place to monitor student activities, staff members will be required to actively monitor student internet usage while in class.

During school, teachers will guide students toward appropriate materials. Outside of school, parents/guardians bear responsibility for such guidance as they do with information sources such as television, telephones, movies, radio and other potentially offensive/controversial media.

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 or other appropriate remedial action.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- Staff users will be issued a login name and password. Staff passwords must be changed periodically.
- Only those network users who have been issued a district-owned device or received prior authorization from the proper District personnel 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 and prohibited.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or District Network Administrator. 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.

IV. Prohibited Activity and Uses

It is not the intention of this Policy to define all inappropriate usage. Inappropriate usage includes but is not limited to:

- 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 the network to engage in harassing or bullying behavior to students to staff.
- 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.

Violation of any of these prohibitions may result in discipline, if applicable, or other appropriate penalties, including suspension or revocation of a user's access to the network.

V. No Privacy Guarantee

Anyone 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. 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, if applicable, suspension and/or revocation of computer access privileges or other appropriate remedial action.

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 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, 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: 9/13/2023