HUDSON CITY SCHOOL DISTRICT **POLICY #4526-R**

(X) Required
( ) Local
(x) Notice

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 by students and staff.

I. ***Administration***

- The Superintendent of Schools will designate a Manager of Instructional Technology to oversee the district's computer network.
- The Manager of Instructional Technology will monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Manager of Instructional Technology will 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 Manager of Instructional Technology, in conjunction with other district administrators, will 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 Manager of Instructional Technology will ensure that all files, disks, attachable drives and software loaded or downloaded onto the computer network have been scanned for computer viruses.
- All student agreements and parental consent forms will be maintained by each the district IT department or designee. ~~to abide by district policy and regulations~~
- All staff agreements and forms to abide by district policy and regulations will be kept on file in the district office ~~to abide by district policy and regulations and forms.~~

II. ***Internet Access***

- The Hudson City School District will make all reasonable attempts to provide Internet access for educational purposes.
- Students will be provided with an individual email account and must only use their district provided email address for use of the school district's network and school district devices.

Unless authorized by the District, the following will be prohibited:

- All users will be prohibited from using the Internet for personal use, including, but not limited to, accessing social networking sites; playing online games; purchasing or selling anything online; accessing personal email services; and watching videos online not related to class assignments.
- Students may not participate in unsupervised online chats not related to instruction.
- Students are not permitted to participate in Google Chat.
- Students may not construct their own web pages or blogs using district computer resources unless authorized by a teacher as part of the curriculum.

Instructional staff members will be required to monitor all of these activities **to the extent possible.**

III. *Acceptable Use and Conduct*

- Access to the district's computer network is provided solely 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 for faculty will be changed every 90-120 days in accordance with the District's password protocol. Passwords for students will be changed once a year.
- 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, vulgar or intimidating language are all inappropriate and unacceptable.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or Manager of Instructional Technology and IT Helpdesk. Under no circumstance should the user forward or share the problem with anyone other than a district official except as authorized by a district administrator.
- 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 activities 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.

- Using the network for commercial activity, including advertising.
- Using district computing resources for commercial or financial gain or fraud.
- 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.
- Stealing data, equipment or intellectual property.
- Using the network to receive, transmit or make available to others obscene, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are discriminatory, racist, sexist, abusive, threatening or harassing to others.
- Accessing another user's account or password without authorization.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and/or deliberately interfering with the ability of other system users to send and/or receive email.
- Forging or attempting to forge email 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.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- 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 another person unless a function of your job duties.
- 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.
- Wastefully using consumable district resources
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other employees and generally accepted network etiquette.
- Removing the current operating system of an assigned device, or adding additional operating system(s) to the same.

V. *Monitoring and Privacy Expectations*

Students and Employees using the district's computer network should not expect, nor does the district guarantee privacy for electronic mail (email) or any use of the district's computer network, even if an email is labeled “confidential” or “private”. The district reserves the right to access and view any material stored or transmitted on district equipment or any material used in conjunction with the district's computer network. The district reserves the right to monitor and audit all technology use, including internet activity, emails, and files stored on or transmitted to or from district devices. Routine maintenance, monitoring and auditing of the district’s technology resources may lead to the discovery that a user has violated this regulation, another district policy, or the law. An individual investigation or search will be conducted if district authorities have a reasonable suspicion that the search will uncover a violation of law or district policy.

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: July 9, 2007
Revision date: June 15, 2021
Revised & Re-Adopted: December 16, 2025