Central Islip Union Free School District

Board of Education & School District Policy Book
50 Wheeler Rd. | Central Islip | N.Y. | 11722
(631) 348-5000
https://www.centralislip.k12.ny.us

Section	Section Title	Type
8000	Support Services	Regulation
Policy	**Policy Title**	
8630-R	Computer Resources and Data Management Regulation	

The following rules and regulations govern the use of the district's computer network system, employee access to the Internet, and management of computerized records. All students and staff are expected to review and understand all aspects of the Acceptable Use Policy located in the District's Technology Plan. The Technology Plan is always available online at **http://www.centralislip.k12.ny.us/techplan**

Administration

- The Superintendent of Schools shall designate the Director of Instructional Technology to oversee the district's computer network.
- The Director of Instructional Technology shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Director of Instructional Technology 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 (1120) taking into account the use of onsite or remote storage.
- The Director of Instructional Technology 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 Instructional Technology 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 (including policy 4526, Computer Use in Instruction) governing use of the district's network.
- The Director of Instructional Technology shall take reasonable steps to protect the network from viruses or other software that would comprise the network.
- All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the Director of Instructional Technology, will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

- Any attempt to bypass Internet filtering and/or monitoring or attempt to bypass the district internet security protocols will be subject to discipline.
- Only approved software (purchased and licensed to the district) will be installed on any district computer. Under no circumstances will personal/unlicensed/unauthorized software be installed on district computers (this includes district laptops).
- Other than the Director of Instructional Technology or his technicians, no users will have any installation rights on any school district computer (this includes school-owned laptops).
- Only computers registered on the Central Islip domain will receive an IP from the server (allowing network/internet access). Staff laptops may have access to the network with written authorization from their Principal/Immediate Supervisor provided the laptop is up to date with a known anti-virus program.

Internet Access

Student Internet access is addressed in policy and regulation 4526, Computer Use for Instruction. District employees and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's computer network.
- Employees are expected to review their e-mail daily.
- Communications with parents and/or students should be saved as appropriate and the district will archive the e-mail records according to procedures developed by the Director of Instructional Technology.
- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use.
- Employees 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. Updated/Additional acceptable use and conduct may be found in the district's technology plan at **http://www.cenralislip.k12.ny.us/techplan**
- All internet traffic over the district's network on any machine/device (including personal computers/devices on the district's network) are subject to internet filtering and monitoring.

Acceptable Use and Conduct

These regulations apply to all staff and third party users (both district-owned hardware/devices and nay personal hardware/device on the district network) 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.
- 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 every 90 days.
- Network users are prohibited from sharing of usernames and/or passwords for any reason.
- Only those network users with permission from the principal or the Director of Instructional Technology 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 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.

Prohibited Activity and Uses

The following is a list of prohibited activity for all staff and third party users (both district-owned hardware/devices and any personal hardware/device on the district network) 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 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.
- 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 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 fraudulent purposes or financial gain.
- 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.
- Use of computer access to data and access to secure areas other than for educational purposes is prohibited.
- Use of any software or hardware to intentionally bypass any district security, firewall, internet filtering or other computer policy/safety measures is strictly prohibited.
- Under no circumstances should any staff or student dismantle or attempt to open a computer for repair or troubleshooting without written authorization from the Director of Instructional Technology.

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.

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.

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.
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.

November 14, 2011
Modified: March 11, 2013