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
4000	Instruction	Regulation
Policy	Policy Title	
4526-R	Acceptable Use Policy Regulation	

The following rules and regulations govern the use of the district's technology and network including access to the internet.

Network and Technology Administration

- The Superintendent of Schools shall designate a district technology administrator (Administrator for Instructional Technology) to oversee the district's technology and network.
- The Administrator for Instructional Technology shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Administrator for Instructional Technology shall be responsible for supporting district policy and regulations governing use of the district's network at the building level with all network users.
- The Administrator for Instructional Technology shall provide employee training for proper use of the network and staff supervising students using the district's network, in turn, will provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The Administrator for Instructional Technology shall ensure that all software installed on the network has been properly purchased and licensed to the district or work in conjunction with special education on “Assistive Technology” installations.
- The Administrator for Instructional Technology shall maintain the district instructional technology inventory.
- The Administrator for Instructional Technology shall be responsible for the administration and integrity of the active directory and group policies.
- The Administrator for Instructional Technology shall be a part of all planning projects for any technology installations.

- The Administrator for Instructional Technology shall review and maintain internet filters for violations or inappropriate access by users.
- Only hardware (computers, tablets, printers, workstations, servers, routers, network switches, etc.) purchased, managed and maintained by the Office of Instructional Technology will be permitted on the district network. Personal hardware (consumer printers, computers, laptops, routers, etc.) will not be maintained nor added to the district's network. Faculty may add personal laptops, tablets, devices to the wireless network using the instructions provided by the Office of Instructional Technology.
- District faculty and staff are prohibited from purchasing and/or receiving (through donation, grant or loan) technology (hardware and software) without the involvement of and written permission from the Office of Instructional Technology. This includes but is not limited to any software, programs, computers, laptops, printers, servers, routers, switches, tablets, iPads, or any other hardware requiring district support.

Internet Access

- Internet access is a privilege and may be revoked for misuse, malicious use, bullying or any infraction against the Policy for District Technology and/or Code of Conduct.
- All staff and students will be provided with a district network account.
- Internet access is for educational and administrative purposes only.
- Internet access is restricted depending on the filtering level of the user.
- The district network is the only acceptable medium for internet access for educational purposes and/or official school business.
- Cyberbullying, social network sites (such as Facebook, Instagram, Pinterest, Tumblr, Reedit, Twitter, Google+, Vine, Snapchat, KiK, YikYak, WhatsApp, Tinder, etc.) that cannot be filtered for inappropriate material are strictly prohibited at all times on the district's network except by authorized district administration for investigative purposes.
- YouTube offers educational filtering to block inappropriate material and will be permitted.
- All faculty and staff will be filtered by the district's internet filter. In the event a teacher or class wishes to do research or work outside of the filter the school Principal can set a bypass using his/her credentials for that specific browsing session.
- District devices (purchased by the district through the Instructional Technology Office) will automatically receive internet/wireless access. Staff may add personal devices or non-district purchased devices to the wireless network for educational purposes using the instructions provided by the Office of Instructional Technology.

The Administrator for Instructional Technology will be required to monitor all internet traffic, activities and network use.

Acceptable Use and Conduct

- Access to the district's technology is provided for educational or administrative purposes and/or for research consistent with the district's mission and goals.
- Use of the district's technology is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Staff and students will never share their personal network credentials or any district usernames/passwords with anyone at any time. All network users are expected to abide by the generally accepted rules of network etiquette (netiquette). This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and obscenities are all strictly prohibited.
- Network users identifying a security problem on the district's network must notify the Administrator for Instructional Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.

Procedures for Proper Use

The following guidelines govern proper use of all district technology.

- The individual in whose name an account is issued is responsible at all times for its proper use.
- Network users will be issued a login name and password. Passwords must be changed periodically. Passwords must follow the guidelines issued by the Administrator for Instructional Technology.
- Only approved software, extension and/or apps (purchased and licensed to the district) will be installed on any district computer, laptop, tablet, mobile device. Under no circumstances will personal, unlicensed, or unauthorized software be installed on district computers (this includes district laptops, tablets and other devices).
- Approved software is defined as software purchased by the Office of Instructional Technology accompanied by a completed software deployment plan and worksheet. Software purchased by individual staff or administrators not approved through the Office of Instructional Technology will not be installed and returned to the vendor.
- Do not leave the account open and unattended.
- Always log off or log out when leaving a computer.

- Other than the Administrator for Instructional Technology or his technicians, no users will have any installation rights on any school district computer (this includes school owned laptops and mobile tablets).

Prohibited Activity and Uses

The following is a list of prohibited activity concerning use of the district's technology. Violation of any of these prohibitions may result in disciplinary or other appropriate penalty.

- Using the network for commercial activity, including advertising. This includes solicitation for non-district sanctioned events, products, services or propaganda using the district email system, website or any other technical resources.
- 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 for any act of bullying or DASA infraction.
- 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.
- Violations of students/staff rights as per FERPA, HIPPA, COPPA and/or CIPA
- 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
- Using district technology resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any district technology resources, or vandalizing the data of another user.
- 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.
- Privately licensed streaming services (Netflix, Amazon Prime, iTunes Music/Movies, Hulu, Showtime, HBO, Starz, etc.) are strictly prohibited for use in education as these services are not under the "Fair Use" law as per the individual license agreements between individual user and service. These copyrighted broadcasts may not be used in public and educational settings and therefore are strictly prohibited on the district network.
- Purchase or receipt of hardware (computers, tablets, printers, workstations, servers, routers, network switches, etc.) without the authorization of the Office of Instructional Technology. Only hardware purchased, managed and maintained by the Office of Instructional Technology will be permitted on the district network. Personal hardware (consumer printers, computers, laptops, routers, etc.) will not be maintained nor added to the district's network. Faculty may add personal laptops, tablets, devices to the wireless network using the instructions provided by the Office of Instructional Technology.

No Privacy Guarantee

All users using the district's technology should not expect, nor does the district guarantee privacy for electronic mail (e-mail) or any use of the district's technology. 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 technology.

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.

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.

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.

Instructional staff should always have alternatives when technology is involved in lesson planning and development in the event of an unplanned outage or hardware failure. Furthermore, instructional staff are strongly urged to fully test all web-based resources prior to use in instruction.

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.

Adopted: February 14, 2011
Modified: April 16, 2018