

Policy 4526

COMPUTER USE IN INSTRUCTION/RESPONSIBLE USE

The Board of Education is committed to optimizing student learning and teaching. The Board considers student 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.

The Board authorizes student use of personal devices to access the district's computer network if the student complies with the district's registration process, as well as the provisions of this policy and regulation. Failure to register or abide by this policy and regulation will result in revocation of access and possibly disciplinary action in accordance with the Code of Conduct.

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.

Regulations and handbooks, to be developed by the Superintendent, in consultation with technology department, 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 as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating the district technology department to oversee the use of district computer resources. The technology department will work with professional development teams to 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 technology department. The technology 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: 5300, Code of Conduct
 5695, Student Use of Personal Electronic Devices

Adoption date:
7/3/17

COMPUTER USE IN INSTRUCTION/RESPONSIBLE USE

The following rules and regulations govern the use of the district's computer network system and access to the Internet.

I. Administration

- The Superintendent of Schools shall designate the technology department to oversee the district's computer network.
- The technology department shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The technology department 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 technology department 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 technology department shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- The technology department 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: before, during, and after school hours
- Students will be provided with individual access accounts
- Students may have Internet access: for educational purposes and other school related activities (ie. Interscholastic sports teams and school clubs)
- Student Internet access may be restricted depending on the grade level.
- In order to access the Internet students must use the district's network
- Students will have individual e-mail address.

A staff member will be required to monitor 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 computer network coordinator, or who have been issued a district-owned device, 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.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or computer network coordinator. 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

The following is a list of prohibited activity 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.
- 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 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.

Regulation 4526-R

- 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

Faculty/staff/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. If a faculty/staff/student is using his/her personal device to access the district's network, the faculty/staff/student must keep school work separate from personal files, since school work is subject to district access. 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 as well as suspension and/or revocation of computer access privileges.

Regulation 4526-R

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:

7/3/17

RULES AND CODE OF ETHICS AGREEMENT FOR STUDENT NETWORK AND INTERNET USERS CARMEL CENTRAL SCHOOL DISTRICT

The Carmel Central School District encourages all staff and students to make use of telecommunications to explore educational topics, conduct research, and contact others in the educational world. Communication over networks, however, should not be considered private and privacy is not guaranteed. Messages may sometimes be accidentally diverted to a destination other than the one intended. Network administration may require review and inspection of directories or messages and the District reserves the right to access stored records. Courts have ruled that old messages may be subpoenaed, network supervisors may examine communications in order to ascertain compliance with network guidelines for acceptable use.

As a technology user, I understand the importance of acceptable use and I agree to follow the Rules and Code of Ethics in all my work with computers in the Carmel Central School District.

- I. I understand and agree to abide by the following Rules and Code of Ethics regarding copyrighted material and intellectual property:
 - A. I recognize that material received via a computer network is owned by the author or the person holding the copyright, and I will give credit to all materials received electronically.
 - B. I recognize that software is protected by copyright laws. Therefore, I will not make copies of software found on school computers, either by copying them onto my own diskettes, USB, or onto other computers through electronic mail or bulletin boards and I will not give, lend, or sell copies of software to others unless I have written permission of the copyright owner or the original software is clearly identified as shareware or in the public domain. Attributions of authorship will follow the same copyright rules for material obtained via the network.
 - C. I recognize that all communications and information accessible via the Internet or the network shall be assumed to be private property of the author and must be documented as such.
- II. I understand and agree to abide by the following Rules & Code of Ethics of use:
 1. Education and curriculum-related research is the first priority of Internet and network use in the Carmel Central School District; all other use is secondary.
 2. Network accounts are to be used only by the authorized owner of account for authorized purposes, using or sharing another student's screen name and/or password is prohibited.
 3. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
 4. No use of the network and/or the Internet shall serve to disrupt the use of the network by others; hardware or software shall not be destroyed, modified, copied, damaged, or abused in any way.
 5. Malicious use of the Internet or the network to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computer systems (e.g., create viruses) is prohibited.
 6. Hate mail, harassment, profanity, obscenity, discriminatory remarks, misrepresentation, libel, impersonation, and other antisocial behaviors are prohibited on the Internet and the network.
 7. Intentional use of the Internet or the network to access or process pornographic material, inappropriate text files, illegal activities, or files dangerous to the integrity of the local area network and its users are prohibited.
 8. Exemplary behavior is expected on "virtual" field trips, as the user is representing the Carmel Central School District when visiting locations on the Internet.
 9. Users shall not reveal their home addresses or phone numbers nor those of others over the Internet. Care must be exercised before revealing a surname over the internet. Similarly, users shall not reveal information about others over the Internet.
 10. Students without signed parental permission to use the Internet are prohibited from teaming up with those who have permission to use the Internet.
 11. Any use of the Internet or the network for commercial for profit or exploitive purposes is prohibited.
 12. E-mail is restricted to users with E-mail accounts authorized by the Carmel Central School District. The use of E-mail shall be governed by all sections of this policy.
 13. Users may not install additional application software or utilities on any school district hardware or make any modifications to school district software, without prior written permission.
 14. I understand that I have the responsibility for my own actions while using the Internet or the network.