

Geneseo CSD Acceptable Use Policy 4526 - R
COMPUTER NETWORK FOR EDUCATION ADMINISTRATIVE REGULATION

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 a computer network coordinator 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.
- The computer network coordinator 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 computer network coordinator 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 computer network coordinator shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- All student and staff agreements and parent/guardian consent forms to abide by district policies and regulations and shall be kept on file in the appropriate building Media Center.

II. Network and Internet Access

- Students will be provided access during instructional time in a controlled environment.
- Students and staff will be provided with individual network accounts. Students in grades K-5 will be provided network accounts at a time determined by their homeroom teachers. All students in grades 6-12 will be required to have network accounts.
- Students and staff may browse the World Wide Web, with the following restrictions:
 - ❖ Students are not to participate in chat rooms or instant messaging services unless they are part of an approved course requirement.
 - ❖ Students may not read news groups without teacher permission.
 - ❖ Students may not construct their own web pages using district computer resources without permission of the webmaster and only under the supervision and/or direction of a staff member or co-curricular advisor.
 - ❖ Students will have individual e-mail address only as needed to meet class assignments and district standards, as set by the Board of Education.
 - ❖ Students are not allowed to belong to mailing lists or listserves, unless they are part of an approved course requirement.
 - ❖ Students may not participate in web journals, message boards or logs without permission of the webmaster and only under the supervision and/or direction of a staff member or co-curricular advisor.
 - ❖ Anytime a staff member requests that a student log off a web site or the network, due to possible access to inappropriate sites or actions, the student must comply or be in violation of the district's "Computer Network Use" policy.

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 must be changed periodically in a time period set by the computer network coordinator.
- Only those network users with written permission from the principal or computer network coordinator 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 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.
- If a student or staff member needs to use any district equipment offsite, including but not limited to flash drives, laptops, projectors, or cameras, s/he will sign a "Receipt of Equipment" document in the technology office or media center.
- If a student or staff member uses portable technology, including flash drives and external hard drives, to store data that could be considered sensitive or confidential, s/he is responsible for the security of this data.

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, as well as having to sign another acceptable use policy.

- Attempting to bypass our network's content filter (we currently use BESS), which restricts access to the parts of the Internet that are deemed appropriate for school use.
- 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.
- 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's 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

Students and staff 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, including flash drives and external hard drives.

VI. Sanctions

All users of the district's computer network and equipment are required to comply with all district policies and regulations governing the district's computer network. Failure to comply with a 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 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 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.