SOUTH SENECA CENTRAL SCHOOL DISTRICT POLICY

4256

COMPUTER NETWORK FOR EDUCATION

The Board of Education is committed to the optimization of student learning and teaching. The Board of Education considers a computer network to be a valuable tool for education and encourages the use of computers and computer-related technology in district classrooms.

The Board encourages computer network use as an integral part of the curriculum. Through software applications, online databases, bulletin boards and electronic mail, the network will significantly enhance educational experiences and provide statewide, national and global communications opportunities for staff and students.

The Board directs the Superintendent of Schools to designate district and building level computer coordination. The computer technology staff working with the curriculum council will make recommendations how to most effectively plan for computers as instructional and learning tools.

The Superintendent shall establish rules and regulations governing the use and security of the district's computer network. Failure to comply with district policy and regulations for use of the network may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Adopted: March 27, 1996

COMPUTER NETWORK FOR EDUCATION REGULATION

The following comprise the rules and regulations relating to the use of the district's computer network system:

ADMINISTRATION

1. The Superintendent of schools shall designate building and district level coordination of the use of computers.
2. Computer technology staff shall monitor activities as deemed appropriate to ensure proper use of the system.
3. The Superintendent coordinates the dissemination and interpretation of district policy and regulations governing use of district's computers at the building level with all users.
4. Computer technology staff shall provide methods to ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.

PROCEDURES FOR PROPER USE

I. The district's computer network shall be used only for educational purposes consistent with the district's mission and goals.
2. The individual is responsible at all times for its proper use.
3. Network users identifying a security problem on the district's system must notify the appropriate teacher, administrator or computer coordinator.
4. Student account information will be maintained in accordance with applicable education records law and district policy and regulation 5500.
5. Copyrighted material may not be placed on any computer connected to the district's network without the author's permission. Only staff specifically authorized may upload copyrighted material to the network.
6. Network users may download copyrighted material for their own use. Copyrighted material shall be used in accordance with the fair use doctrine and district policy and regulation 8650.
7 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.

PROHIBITIONS

The following is a list of prohibited actions concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalties, including suspension or relocation of a user's access to the network.

1. There must be no sharing of passwords.
2. Attempts to read, delete, copy or modify the electronic mail of other system users is prohibited as is deliberate interference with the ability of other system users to send/receive electronic mail. Forgery or attempted forgery of electronic mail messages is prohibited.
3. No personal software or disks may be loaded onto the district's computers and/or network without permission of the administrator.
4. Attempts to log on to the district's system in the name of another individual with or without the individual's password is prohibited.
5. Use of computer access to data and access to secure areas other than for educational purposes is prohibited
6. Transmission of material information or software in violation of any district policy or regulation, local, state or federal law or regulation is prohibited.
7. Vandalism will result in cancellation of system use privileges. Vandalism is defined as a malicious attempt to harm or destroy district equipment or materials, data of another user of the district's system or any of the agencies or other networks that are connected to Internet. This includes, but is not limited to, the uploading or creating of computer viruses.
8. Tampering with or misuse of the computer system or taking any other action inconsistent with this policy and regulation will be viewed as a security violation.