Gowanda Central School District
Board of Education Policy

4510.1

INSTRUCTIONAL TECHNOLOGY

The Board of Education recognizes its responsibility to ensure that district staff and students have access to up-to-date technological materials and equipment. As used in this policy, "technology" refers principally to electronic materials and equipment, such as computers, telecommunications, lasers and robotics, as available.

The following reflect the district's goals for students regarding instructional technology:

1. to foster an atmosphere of enthusiasm and curiosity regarding new technology and its applications;
2. to heighten each student's familiarity and/or working knowledge of current technological materials/equipment;
3. to provide equal access to district technological materials/equipment and to instruction in their implementation;
4. to ensure that the various technologies are utilized in a variety of applications, and are not restricted to one subject area or one location in the schools; and
5. to promote district educational goals through the use of such technology(ies).

In order to achieve the above-stated goals, the Board shall seek the advice of representatives from groups utilizing technology in pursuit of district goals (i.e., Board members, administrators, teachers, support staff, parents, and students). In addition, the Board directs the Superintendent of Schools to equip district schools with appropriate and up-to-date hardware/software, to schedule "hands-on" inservice activities for district staff, and to implement suggestions from the above representatives and Director of Technology, within budgetary constraints.

Gowanda Central School District
Board of Education Policy

COMPUTER NETWORK FOR EDUCATION 4526

The Board of Education is committed to the optimization of teachers and student learning and teaching. The Board 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 a technology coordinator to oversee the use of district computer resources. The technology coordinator will prepare programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent, working in conjunction with the designated Purchasing Agent for the district, the technology coordinator and the District Technology Curriculum Team, 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.

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.

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 a computer coordinator to oversee the district's computer network.
2. The computer coordinator shall monitor and examine all network activities as deemed appropriate to ensure proper use of the system,
3. He/She shall disseminate and interpret district policy and regulations governing use of the district's network at the building level with all network users.
4. He/She 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 copies of district policy and regulations governing use of the district's network.
5. He/She shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
6. All student agreements to abide by district policy and regulations shall be kept on file in the district office.

System Access

The following individuals may be designated as members with access to the computer network system:

1. Elementary, middle and secondary students maybe granted an account for up to one academic year at a time.

2. Teachers may apply for an individual and/or a class account.
3. Other district employees as deemed necessary.
4. Community members as deemed necessary.

Procedures for Proper Use

1. The district's computer network shall be used only for educational purposes consistent with the district's mission and goals.
2. The individual in whose name an account is issued is responsible at all times for its proper use.
3. Network users will be issued a login name and password. Passwords must be changed every 30 days.
4. Only those network users with written permission from the there supervisor and computer coordinator may access the district's system from off-site (e.g., from home).
5. Network users identifying a security problem on the district's system must notify the appropriate teacher, administrator or computer coordinator. Do not demonstrate the problem to anyone.
6. Student account information will be maintained in accordance with applicable education records law and district policy and regulations 5500.
7. 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.

8. 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 regulations 8650.

9.Any network user identified as a security risk or having a history of violations 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 penalty, including suspension or revocation of a user's access to the network.

1. There must be no sharing of passwords without written permission from the teacher/administrator or computer coordinator, as appropriate.
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 teacher/administrator or computer coordinator.
4. Attempts by a student to log on to the district's system in the name of another individual, with or without the individual's password, is prohibited.
5. System users shall not encourage the use of tobacco, alcohol or controlled substances or otherwise promote any other activity prohibited by district policy, state or federal law.
6. Use of computer access to data and access to secure areas other than for educational purposes is prohibited.
7. System users shall not evade, change or exceed resource quotas as set by the administration. A user who continues to violate disk space quotas after seven calendar days of notification may have their file removed by the system coordinator. Such quotas may be exceeded only by requesting to the appropriate administrator or system coordinator that disk quotas be increased and stating the need for the increase.
8. Transmission of material, information or software in violation of any district policy or regulation, local, state or federal law or regulation is prohibited.
9. 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 the Internet. This includes, but is not limited to, the uploading or creating of computer viruses.
10. 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.

STUDENT INTERNET CONTENT FILTERING/SAFETY POLICY
THE CHILDREN'S INTERNET PROTECTION ACT

In compliance with The Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the District has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. Further, appropriate monitoring of online activities of minors, as determined by the building/program supervisor, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the Board of Education's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate teaching/instructional materials and activities to enhance the schools' programs; and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web *may* include, but shall not be limited to, the following guidelines:

a) Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail and chat rooms may be blocked as deemed necessary to ensure the safety of such students;

b) Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors;

c) The dissemination of the District's Acceptable Use Policy and accompanying Regulations to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet. In compliance with this Internet Safety Policy as well as the District's Acceptable Use

Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and

d) Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal information regarding such students.

The determination of what is "inappropriate" for minors shall be determined by the District and/or designated school official(s). It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measure," "sexual act," and "sexual contact" will be as defined in accordance with CIPA and other applicable laws/regulations as may be appropriate and implemented pursuant to the District's educational mission.

Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the School District.

The School District shall provide certification, pursuant to the requirements of CIPA, to document the District's adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking/filtering of access to certain material on the Internet) for all School District computers with Internet access.

Internet Safety Instruction

In accordance with New York State Education Law, the School District may provide, to students in grades K through 12, instruction designed to promote the proper and safe use of the Internet. The Commissioner shall provide technical assistance to assist in the development of curricula for such course of study which shall be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the internet.

Notification/Authorization

The District's Acceptable Use Policy and accompanying Regulations will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet. Student access to District computers is conditioned upon written agreement by the student and his/her parent acknowledging that the use will conform to the requirements of the District's Acceptable Use Policy. All agreements shall be kept on file in the District office. The District has provided reasonable public notice and has held at least one (1) public hearing or meeting to address the proposed Internet Content

Filtering/Safety Policy prior to Board adoption. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of the District's Internet Content Filtering/Safety Policy, as well as any other District policies relating to the use of technology.

47 United States Code (USC) Sections 254(h) and (I)
47 Code of Federal Regulations

1st reading: June 5, 2013
Public Forum: June 5, 2013
Approval: June 5, 2013