Policy #6435

NETWORK AND INTERNET ACCEPTABLE USE POLICY
SCHOOL DISTRICT OF SENECA

The Seneca District Schools is providing access to a computer network and the Internet as a means to enhance the curriculum and learning opportunities for all of its students and staff. The District has established this policy, the Network and Internet Safety Policy, the Web Page Policy, Bullying / Cyber Bullying / Harassment to ensure appropriate use of these resources. Use of the District's computers, peripherals, Network and Internet access shall be viewed as a privilege, not a right.

The reasons for using the Network and the Internet as instructional resources are:

- access global information resources.
- utilize electronic mail (e-mail) for communication.
- enter into partnerships to enhance learning options.
- broaden problem-solving and decision-making abilities.
- broaden research capabilities by using appropriate materials.
- develop higher level thinking skills.
- gain skills needed for the 21st century.

On the Internet, it is impossible to control all materials. Some users may discover educationally unsuitable information. Through the Internet, students may have access to materials that are illegal, defamatory, inaccurate or potentially objectionable to some people. However, the District believes that the educationally appropriate information and interaction available on this worldwide network outweighs the possibility that users may procure materials that are not consistent with the educational goals of the District. The Acceptable Use Policy will serve as the guide to foster appropriate use of the Internet. Staff supervision, training, technology protection measures and the monitoring of online activities of minors are measures the School District of Seneca will take to restrict minors' access to materials harmful to minors, minimize the chances of users accessing unsuitable sites or material via the Internet or other forms of electronic communications and to see that the Internet, network and computer equipment and peripherals are being used in compliance with this policy, the Network and Internet Safety Policy, the Web Page Policy and the Bullying / Cyber Bullying / Harassment Policy.

Cyber bullying includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate and/or hurtful e-mail messages, instant messages, text messages, digital pictures or images, or web site postings, including blogs. It is also recognized that the author (poster or sender) of the inappropriate material is often disguised (logged on) as someone else. In addition, any communication of this form that disrupts or prevents a safe and positive educational or working environment may also be considered cyber bullying.

The District will provide instruction in standards of Internet safety as part of its PK-12 Cybersmart curriculum. In addition, just-in-time instruction as needed, for the use of specific tools in the regular classroom will be provided. The instruction will include appropriate use of social networking sites and communication tools, safeguarding personal information online, how to recognize Internet predators, how students should respond to cyber bullying and the district's policy on cyber bullying and online harassment. In addition, as specific Web 2.0 tools are used in individual classrooms, instruction for proper behavior and etiquette when using

those tools will be provided.

All users of the Network and the Internet should be aware that the inappropriate use of electronic processing and information resources can be a violation of local, state and federal laws. Violations can lead to prosecution. When using the District's access to the Internet, users are expected to abide by the policies established by this policy, the Network and Internet Safety Policy, the Web Page Policy and the Bullying / Cyber Bullying / Harassment Policy. Unacceptable use of the system will result in the suspension or revocation of Internet and network use and/or appropriate disciplinary actions per the Log Card System. As the use of the network and the Internet is a privilege and not a right, the user will be held responsible for her/his actions using District technology, the Internet and/or the Network.

When using the District's computers, peripherals, Network and Internet access, users are expected to abide by the policies established by the District, which include generally accepted rules of network etiquette and cyber safety. These include (but are not limited to) the following:

Acceptable Use
Responsible Users:
- may use the Internet to research assigned classroom projects.
- when supervised by professional staff, may use the Internet to send electronic mail (e-mail) to other users for educational and research project purposes.
- when supervised by professional staff, may use the Internet to participate in chat rooms for educational and research project purposes.
- when supervised by professional staff, may use the Internet to send instant messages or other forms of electronic communications to other users for educational and research project purposes.
- may use the Network to send Intranet electronic mail (e-mail) to other District users.
- may use the Internet to explore other computer systems.
- will respect and uphold copyright laws and all other applicable laws or regulations.
- will respect the rights and privacy of others by not accessing private files.
- will follow all regulations posted in the computer labs or other rooms where computers are in use.
- will follow the directions of the adult in charge of the computer labs or other rooms where computers are in use.

Unacceptable Use

Responsible users:
- shall NOT use the Internet for any illegal purpose or activities.
- shall NOT use the Internet or network for unauthorized access, including 'hacking' and other unlawful activities.
- shall NOT use impolite or abusive language.
- shall NOT harass any Internet or network user.
- shall NOT plagiarize works they find on the Internet.
- shall NOT use the District system to access material that is profane or obscene (pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made if the purpose is to conduct research and access is approved by both the teacher and the parent. District employees may access the above material only in the context of legitimate research.

- shall NOT use network facilities for fraudulent copying, communications or modification of materials in violation of copyright laws. The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to “fair use” guidelines.
- shall NOT violate the rules of common sense and etiquette.
- shall NOT use the network for non-education related activities.
- shall NOT use the network to transmit material likely to be discriminatory, offensive or inflammatory communication (cyber bullying).
- shall NOT change any computer files that do not belong to the user.
- shall NOT use the system for commercial use or for-profit purposes.
- shall NOT use an account other than their own or misrepresent their identity.
- shall NOT create and/or distribute a computer virus, worm or Trojan horse over the network.
- shall NOT use the system to illegally transfer software, otherwise known as pirating.
- shall NOT reveal personal identification information about themselves, other students or staff.
- shall NOT use the network in such a way that they would disrupt the use of the network by other users.
- shall NOT deliberately or willfully cause damage to computer equipment and/or peripherals or assist others in doing the same.
- shall NOT deliberately access materials that are inconsistent with the school’s code of conduct or district’s educational goals or show others how to do the same.

In the event there is an allegation that a student has violated this policy, Network and Internet Safety Policy, the Web Page Policy and/or the Bullying / Cyber Bullying / Harassment Policy, the student will be given an opportunity to be heard by the Technology Coordinator and Disciplinary Officer. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Employee violations of the District Acceptable Use Policy will be handled in accordance with District policy and the employee handbook.

Users should be aware that the use of the network, the Internet and/or email is not guaranteed to be private. System operators will have access to all user accounts, including e-mail. Messages relating to or in support of illegal activities will be reported to the proper authorities.

Each student, community education participant and staff member needing to use a Network account and/or the Internet shall be assigned a network account and Internet access privileges upon the signing of an agreement to abide by this policy, the Network and Internet Safety Policy and the Web Page Policy. Only those minor students, grades Pre-K through 12, with written parental permission slips will be authorized access to the Network and Internet.

6.3 Students are Responsibilities for:

Using computers/devices in a responsible and ethical manner.
Obeying general school rules concerning behavior and communication that apply to Chromebook/computer use.
Using all technology resources in an appropriate manner so as to not damage school equipment. This “damage” includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by the student’s own negligence, errors or omissions. Use of any information obtained via Seneca School District’s designated

Internet System is at your own risk. Seneca School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
Helping Seneca School District protect our computer system/device by contacting an administrator or a facilitator about any security problems they may encounter.
Monitoring all activity on their account(s).
Students should always turn off and secure their Chromebook after they are done working to protect their work and information.
If a student should receive email containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to print a copy and turn it into the office.
Returning their Chromebook to the facilitator at the end of each school year. Students who withdraw, are expelled or terminate enrollment at Seneca for any other reason must return their individual school Chromebook on the date of termination.

6.4 Student Activities Strictly Prohibited:
Illegal installation or transmission of copyrighted materials.
Any action that violates the Student Handbook, existing Board policy or public law.
Sending, accessing, uploading, downloading or distributing offensive, profane, threatening, pornographic, obscene or sexually explicit materials.
Unauthorized use of chat rooms, sites selling term papers, book reports and other forms of student work.
Internet/computer games (non-school initiated).
Use of external attachments without prior approval from the facilitator.
Changing of Chromebook settings (exceptions include personal settings such as font size, brightness, etc).
Spamming-Sending mass or inappropriate emails.
Gaining access to other student's accounts, files and/or data.
Use of the school's internet for financial or commercial gain or for any illegal activity.
Use of anonymous and/or false communications using messenger services (Ex. – MSN Messenger, Yahoo Messenger, etc.)
Students are not allowed to give out personal information over the Internet without supervisor's approval. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, Ebay, email, etc.
Participation in credit card fraud, electronic forgery or other forms of illegal behavior.
Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
Bypassing the Seneca web filter through a web proxy.

- Students may access the Internet only through the district's wireless public network, which provides filtered Internet access. The school district does not condone the use of other Internet connection methods such as 3G/4G data plans, and is not responsible for any accrued data charges.
- Students and their families assume responsibility for their device. The school district is not responsible for the safety, security, loss, theft, damage or misuse of any personal device. The school district recommends that the device is stored in a locked locker

when not in the student's possession.

- Students and their families assume responsibility for the technical support and maintenance of personally owned devices, including troubleshooting and repair costs.
- Students and their families assume responsibility for any desired insurance for their personal device.
- Students will never use their personal device in locker rooms, restrooms or any other area where personal privacy is a concern.