SUBJECT: COMPUTER USAGE AND INTERNET SAFETY

This policy describes the requirements of users regarding the acceptable use of information technology in the Susquehanna Valley School District. The Susquehanna Valley School District makes available a variety of technological resources to support learning and enhance instruction. The goal of the Susquehanna Valley School District is to provide access to information technology to facilitate resource sharing. innovative instructional opportunities, and communication. The users of Susquehanna Valley School District Information Technology assume certain responsibilities and agree to abide by the rules and regulations listed below, including the use of technology in an ethical manner and under applicable legal provisions.

In accordance with the Child Internet Protection Act (CIPA) Internet activity on Susquehanna Valley School District networks is electronically filtered and monitored. Access to Internet sites and services is filtered to limit access to inappropriate content (i.e., pornography, P2P networks, hate groups, violence, illegal activities, extremist groups and cults, online advertising, etc.) to the highest degree possible. However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Internet activity is logged and monitored in accordance with Federal Communications Commission (FCC) for participation in the federal E-rate program to help assure the safety and security of students and staff.

Scope

This policy applies to all student and staff users including full-time and part-time employees, temporary workers, volunteers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of the Susquehanna Valley School District.

Definitions

a) Information system - A network, server, desktop computer, laptop, personal digital assistant (PDA), peripheral, printer, electronic media, electronic messaging systems (i.e., e-mail), program, database, or related hardware or software that is owned, developed, managed, operated, maintained, or used by the Susquehanna Valley School District.

b) Sensitive Information - Private information such as health, financial, student, and personnel data that is protected by law from public disclosure or unauthorized access, and other information for which protection is required based on confidentiality agreements, policies, or similar requirements.

c) User - An individual who uses a Susquehanna Valley School District information system and/or electronically accesses, views, creates, processes, modifies, stores, or transmits Susquehanna Valley School District information.

d) Other Networks - Other school districts network (i.e., Broome-Tioga BOCES), vendor networks and/or web programs.

(Continued)

SUBJECT: COMPUTER USAGE AND INTERNET SAFETY (Cont'd.)

Policy

Users will use Susquehanna Valley School District information systems for authorized purposes only. The Susquehanna Valley School District monitors its information systems and has put into place processes and controls to safeguard the information stored, transmitted, and displayed on its information systems. The information systems are the property of the Susquehanna Valley School District and users should have no expectation of privacy.

Users are expected to:

a) Respect the privacy of others and security of the Susquehanna Valley School District System.

1. Users will use only the login credentials (i.e., user IDs) issued to them by the Susquehanna Valley School District.

2. Users will not share the passwords provided or assigned to them with other individuals.

3. Users will not try to learn passwords of other users or information system administrators.

4. Users will not access, store, or cause to be transmitted offensive, hateful, harassing, insulting, false or defamatory, sexually explicit, obscene, or otherwise inappropriate information via Susquehanna Valley School District information systems.

5. Users will not use information systems in a way that will preempt the work activities or duties of others.

b) Respect the legal protections to programs and data provided by copyright and license.

1. Users will not copy, download, install, or distribute licensed software in violation of copyright laws or licensing agreements.

2. Users will use copyrighted materials in accordance with the "fair use" doctrine (17 United States Code (USC) Section 107) and will not copy, distribute, or transmit a third party's information in violation of copyright laws.

c) Respect the integrity of Susquehanna Valley School District information systems and other networks to which the District is connected.

(Continued)

SUBJECT: COMPUTER USAGE AND INTERNET SAFETY (Cont'd.)

1. Users must not conceal their identity when using the Susquehanna Valley School District System, except when the option of anonymous access is explicitly authorized.

2. Users will not install on or connect to Susquehanna Valley School District information systems any personally-owned or a third party's software, computer equipment, peripheral, or network connection without authorization. Users may use a personally-owned computer to connect to Susquehanna Valley School District information systems made available for access via the Internet; however, users will not store Susquehanna Valley School District information on any such system without authorization.

3. Users will not bypass any security system or feature put in place to protect, monitor, or restrict access to information or Susquehanna Valley School District System information systems (e.g., using a proxy server to access a Web site blocked by Susquehanna Valley School District System content filters).

4. Users will not create, download, install, or use software or equipment to test the weaknesses of, infiltrate, circumvent, provide "back door" access to, or cause damage to information systems.

5. Users will not remove or make modifications to information systems, or copy or make changes to system configuration files, without authorization.

6. Users will not use unauthorized software, devices, or settings (e.g., disabling remote access or installing an unauthorized encryption program) to prevent authorized individuals from accessing information or information systems.

d) Use Susquehanna Valley School District information systems for authorized purposes only.

1. Users will not attempt to gain unauthorized access to, disrupt, interfere with, or destroy information or information systems.

2. Users will not use Susquehanna Valley School District information systems for unauthorized purposes including, but not limited to, playing games unrelated to academic activities; personal business endeavors; illegal purposes or activities in violation of civil or criminal laws at the federal, state, or local levels (e.g., promoting a pyramid scheme, distributing illegal obscenity, infringing copyrights, making bomb threats, solicitation or lobbying activities, discriminatory activities, cyber bullying [refer to policy 7552], receiving, transmitting, , or possessing child pornography); or other activities prohibited by Susquehanna Valley School District policy.

(Continued)

SUBJECT: COMPUTER USAGE AND INTERNET SAFETY (Cont'd.)

3. Users will limit incidental personal use not related to work. Incidental personal use is permitted only during duty-free time and only if the use has no tangible impact on the function of Susquehanna Valley School District information systems and the use otherwise conforms to the requirements of this policy.

4. Users will not waste information system resources including computer processing time and storage, network capacity, and information technology supplies provided by the Susquehanna Valley School District (e.g., storing large amounts of music, video or picture files, downloading music, video, and picture files, playing computer games, sending or receiving large amounts of non-work related e-mails, etc.).

e) Protect Susquehanna Valley School District information from loss, theft, unauthorized disclosure, or unauthorized use.

1. Users will not share or enable unauthorized individuals to access private information of the Susquehanna Valley School District including but not limited to sensitive information related to students and employees.

2. Users will not transfer or transmit sensitive information to another individual without explicit authorization. When authorized, users will apply appropriate safeguards to prevent unauthorized access to the information.

3. Users will not share information with other individuals that could allow those individuals to gain unauthorized access to information systems of the Susquehanna Valley School Districts System. Users will not use personal electronic messaging accounts not provided by Susquehanna Valley School District for any official Susquehanna Valley School District System communication.

4. Users will take appropriate precautions to safeguard the information and information systems assigned to them, on and off Susquehanna Valley School District premises, to prevent loss, theft, damage, or unauthorized use.

5. Users will promptly report any known or suspected loss, theft, unauthorized disclosure, or unauthorized access to the Director of Technology.

6. Users aware of an alleged violation of this Computer Usage and Internet Safety Policy and who may or may not have been harmed by the alleged violation may report the matter to the Director of Technology.

(Continued)

SUBJECT: COMPUTER USAGE AND INTERNET SAFETY (Cont'd.)

Sanctions

A violation of this Susquehanna Valley School District policy may lead to corrective action pursuant to the provisions of District policy, applicable contracts and/or agreements. Under certain circumstances, violations of this Susquehanna Valley School District policy may give rise to civil and/or criminal liability. Users may be subject to criminal prosecution, civil liability, or both for the unlawful use of any internet technology resource outside the jurisdiction of the Susquehanna Valley School District System. The Susquehanna Valley School District may also pursue legal action as deemed appropriate against individuals for unauthorized access, use, or destruction of information assets or for any use which violates copyrights or licensing laws, regulations, or contracts. Users whose access privileges are revoked, suspended or limited as a consequence of a violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the formal appeals provisions of the relevant disciplinary authority and/or provisions of applicable contracts.

NOTE: Refer also to Policies #7552 -- Bullying: Peer Abuse in the Schools
#8271 -- Children's Internet Protection Act: Internet Content Filtering/Safety Policy

Adopted: 6/15/11
Revised and Adopted 7/11/12