Southwest Vermont Regional Technical School District	**TELECOMMUNICATIONS AND NETWORK POLICY**	Policy # 6140C **[Required]**

It is the policy of the Boards of Directors of the Southwest Vermont Regional Technical School District (**referred to elsewhere in this document as** SVRTSD) that staff and students will use all SVRTSD telecommunications and network equipment solely for appropriate educational purposes.

The purpose of the Telecommunications Network Policy is to help protect the SVRTSD and its employees and/or students from liability due to inappropriate use of computers, network, and other telecommunications equipment and breaches of computer security. This policy is not intended to address every computer operating, telecommunications and security issue. It is the user's responsibility to exercise sound judgment.

The attached Administrative Regulations are subject to change at any time.

	Date Drafted	Date Warned	Date Adopted
Southwest Vermont Regional Technical School District	12/03/07	12/17/07	1/15/08

Administrative Regulations for
Telecommunications and Network Policy # 6140C:

Table of Contents

I.Computer Users

Computer users are responsible for the appropriate use of CDC computers and other equipment, and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of CDC computer equipment, breaches of computer security, and assisting in resolving such matters. Users are responsible for adhering to CDC policies and practices as described herein, and in other CDC policy manuals, to ensure CDC computers are used in accordance with policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment.

a. Unauthorized Access

Unauthorized access of CDC computers is prohibited. Unauthorized access of third-party computers via CDC computers is prohibited. Attempting to access CDC computers or data without specific authorization is prohibited. Any form of tampering, including but not limited to snooping and hacking, to gain access to computers is a violation of CDC policy and federal law, and carries serious consequences. Employees are required to turn their computer off at the end of the day, and when not in use for an extended period of time. This will help prevent computer security breaches, and damage due to power surges. In addition, computer users must take other reasonable precautions to prevent unauthorized access of computers.

b. Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of CDC computers, programs, files, or data is prohibited and will be investigated and prosecuted to the fullest extent of the law.

c. Passwords

Your participation is crucial to effective computer security. Not only the CDC is at risk when someone gets your password. Computers often contain confidential information. If this information is accessed and distributed, it could cause great harm to you or someone you work with (i.e. Students). Once someone gets your password, they have the capacity to, among other things:

¨ Send e-mail to individuals, or groups, representing themselves as you

- Disseminate your files over the Internet
- Delete or alter files
- Monitor your work

d. Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from snoopers. A lot of damage can be done if someone gets your password. Users will be held accountable for password selection and protection.

Do not share your password with anyone, other than a designated Technology Services Department official. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line. You are required to report any bios password to the Technology Services Department immediately.

Poor password selection and safekeeping is not comforting to administration investigating a computer security breach, nor is it an acceptable excuse if a hacker damages CDC computer systems using your password.

e. Easy to Remember and Hard to Crack

Another concern is forgetting your password. Getting into your computer when you have forgotten the password is, in some cases, very difficult. Good methods to help you remember your password is to select a password that is unique to you, and try to use it at least once every day. For example, if you live on Elm Street, do not select “elm” as a password. Select the nearest crossroad and always finish, or start, with a number (maybe your youngest child’s age).

The following is a good guideline for password selection:

- Use 5 or more characters, and at least one numeric character
- Your password should not include your login name, your name, your spouse’s or partner's name, children’s or pet's name, or any other names commonly known to others
- Your password should not be a word pertaining to the CDC, your work, or an activity that you participate in or follow that is commonly known
- Your password should not include anything derogatory, offensive, or defamatory

If you have a question about password selection or safekeeping, please contact the Technology Services Department.

f. Password Access Program

The CDC’s password access program is an excellent tool to defend against unauthorized access of CDC computers. However, a password access program is only effective when used properly.

Do not leave your computer logged on and unattended for an extended period of time. Do not log on to your system if someone can see you keying in your password (there is no need to create the temptation). Turn off your computer when you leave at night. If you use a remote access program; such as, R LINK, and you need to leave your computer on, be sure that it is properly secured and supervised. Furthermore, use a screen saver access program to secure the computer from unauthorized access. (Make sure to inform Technology Services Department of your password and only Technology Services Department should know your password.)

g. Snooping and Sniffing

Snooping -- Defined in Webster's Dictionary as "to pry about in a sneaking way."
Sniffing – interception of data

Snooping and/or sniffing into CDC computer systems is a serious violation of policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to administration. Watching other users enter information, and looking at computer disks that do not belong to you, are prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of CDC policy. If you observe someone snooping, report it to administration.

h. Hackers

Hackers are working hard to break into computer systems. They alter and delete files, and cause other havoc for fun or profit. A common exposition of hackers prosecuted for criminal activity is that they felt computer systems' weaknesses exist to be exploited.

Hackers frequently penetrate computer systems by calling unsuspecting employees representing themselves as a new employee, executive of the CDC, or another trusted individual. Through a variety of probing questions, they obtain the information necessary for their hacker programs to do their work.
Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and tell them you will get right back to them. Report the incident immediately to administration and Technology Services Department. Without your help, the Technology Services Department has little chance of protecting our computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using CDC computers is prohibited, and will be reported to the local authorities. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. If you are caught hacking, it is a serious offense. If you identify vulnerability in the CDC's computer security system, report it to administration and to the Technology Services Department.

i. Viruses, Worms and Trojan Horses

It is critical that users make certain that data and software installed on CDC computers are free of viruses. Data and software that have been exposed to any computer, other than CDC computers, must be scanned before installation. This includes e-mail with attachments (a virus can quickly contaminate your computer simply by opening an e-mail attachment), downloads from the Internet and other sources of data that may be contaminated. Viruses can result in significant damage, and lost productivity. Therefore, all software needs to be installed by the Technology Services Department, which will scan for viruses before installation.

Use of virus, worm, or trojan horse programs is prohibited. If you identify a virus, worm, or trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the Technology Services Department. The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. They easily travel down phone, cable, ISDN, or other communication lines, infect e-mail, data and files, and find their way to other computer systems. The key to containment is limiting the reach of the contamination. Turning off your computer does this best.

II.Confidentiality

a. General

All computer information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited, without prior administration approval.

b. Handling Confidential Information

Confidential information stored on computers is typically more difficult to manage then traditional paper documents that are sealed in an envelope, and locked in a filing cabinet clearly labeled CONFIDENTIAL. As such, it is important that users take extra care with confidential information stored on computers. The following are inappropriate under normal circumstances when dealing with confidential information:

- Printing to a printer in an unsecured area where documents may be read by others
- Leaving your computer unattended with confidential files logged on to your system
- Leaving computer disks with confidential data unattended, in easy to access places. Remember it only takes a minute to copy a disk
- Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from administration and information systems administration.

c. Encryption

Encryption and encryption utilities are prohibited without administration approval. If you need to send confidential or proprietary information over the Internet, or other public communication lines, you must obtain prior approval from administration.

III. Physical Security

Computer Theft

a. Locks

Physical security is key to protecting your computer and computer information from loss and damage. Store floppy disks and other sensitive information in a secure place. Turn off your computer when it is not in use for an extended period of time. Lock the door to your office/classroom, if you have one. Take a few minutes to practice good physical security. Your investment of time will provide an excellent return, and help prevent temptation by others.

b. Laptops

There is no sure way to secure laptops. However, there are many sensible, cost-effective measures that can help reduce the risk of loss or damage. The following are required when taking laptops off CDC property:

- Laptops must be signed out
- When you sign out a laptop you are taking personal financial responsibility for the replacement and/or repair costs for the laptop in the event of loss or damage, with the exception of normal wear & tear
- Report lost or stolen computers immediately
- All important files must be backed-up, and back-up disks must be stored in a separate physical location from the computer
- Confidential, important, and proprietary data leaving the facility requires administration authorization
- Use reasonable precautions to safeguard the laptop against accidental damage (don't work on your laptop in the pool)
- When traveling, laptops must be in sight at all times or physically secure
- Always store laptops in a concealing carrying case

c. Off-Site Computers

Off-site users must take additional precautions to safeguard computer information and equipment, including but not limited to:

- Safeguarding the computer and information from theft or damage
- Prohibiting access to the computer (including family, friends, associates, and others) for any purpose, without administration authorization
- Adhering to all computer policies and practices of the CDC for on-site users

I.

II. Administrative Matters

a. Back-up

Only you can prevent data loss!

Users are responsible for regular back up of essential computer files, and secure storage of back-up disks.

Backing up files is key to productivity, and safeguarding data against unwanted intrusions. Important files should be backed-up daily. Decisions about what to back up, and how often to back-up, should be considered with one simple thought in mind. How much productivity would be lost if your computer were stolen? So much work is done in a single day, that in most cases, it is irresponsible to not take a few minutes to back-up essential data.

All backed-up files should be stored on a secure computer disk or tape, other than the one containing the original data. The back-up disk or tape should be stored on site, preferably in a secure place.

All important, confidential, or proprietary information must be stored on the local area network (LAN). Storing information of this type on your desktop computer is prohibited without authorization from administration. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering, and other security breaches. Maintenance and back up are performed on the LAN daily. Programs and other information are updated on the LAN regularly. Use the LAN; it is safe, effective, and reliable.

b. Copyright Infringement *(refer also to copyright policy # 6130C)*

The CDC does not own computer software, but rather licenses the right to use software. Accordingly, authorized CDC officials in accordance with the terms of the software licensing agreements may only reproduce licensed software. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well. There is no "but copying it was so easy" defense to copyright infringement. Copyright infringement is serious business, and the CDC strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with administration immediately.

Copies of shareware or "free" programs must be registered with the Technology Services Department. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a "donation," often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for "free" software to contain a virus. As such, it is important that all new software is registered with the Technology Services

Department. Your supervisor and the Technology Services Department must approve requests for application programs.

c. Harassment, Threats and Discrimination

(Refer also to student and employee harassment policy # 4001C & 5002C)

It is CDC policy, and the law, that employees and students are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment.

It is not uncommon for employees and/or students to receive files, data, pictures, games, jokes, etc., that may be considered offensive by some. Currently, there are many cases in the courts addressing just such issues, the ramifications of which are significant. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Stay away from such activity; it is a serious violation of CDC policy. It is inappropriate to use CDC computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside the school.

d. Unauthorized Changes to CDC Computers

Installing software and making changes to computer hardware, software, system configuration, and the like are prohibited, without Technology Services Department authorization. The CDC computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems ultimately result in lost productivity. Such changes often require a computer technician to fix both the original problem, and the problem caused by the would-be computer technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computer systems.

The following are just a few examples of changes to computers that can result in operating problems:

1. Installation of any hardware, commercial software, shareware, and free software. Some software requires an upgrade of computer hardware, the operating system, or both for the program to operate properly. Some programs are simply not written well, and can cause problems with the computer
2. Installation of some programs changes the computer's system configuration, which can result in problems with your computer
3. Data used on home computers may become infected with a virus, and contaminate your computer and other CDC computers

The list of potential problems goes on and on. Accordingly, get approval from Technology Services Department before making any changes to CDC computers.

e. Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from Technology Services Department. All computer software and hardware purchases must be registered with the Technology Services Department, meet pre-established quality requirements, and be compatible with other CDC computer software and equipment.

f. Personal Use of Computers

Incidental and occasional personal use of CDC computers is permitted for reasonable activities that do not need substantial computer hard disk space, or other computer equipment. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of CDC computers. Prohibited activities include, but are not limited to, computer games, personal software and hardware, writing your autobiography, and running a personal business on the side. Using CDC computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor. Personal files, information, and use of CDC computers will be treated no differently by the CDC than business use, with regard to employee and/or student privacy.

Many software games are illegally copied, and often contain viruses. Such programs represent a potential liability to you and the CDC. Proof of ownership and administration authorization for use is required for all software on CDC computers.

g. Reporting Policy Violations

Employees are required to report violations, or suspected violations, of computer policy. Activities that should immediately be reported to administration include, but are not limited to:

4. Attempts to circumvent established computer security systems
5. Use, or suspected use, of virus, trojan horse, or hacker programs
6. Obtaining, or trying to obtain, another user's password
7. Using the computer to make harassing or defamatory comments, or to in any way create a hostile work environment
8. Using the computer to communicate inappropriate messages or jokes that may be considered offensive by others
9. Illegal activity of any kind

Computer policy violations will be investigated. Noncompliance with the CDC Telecommunications Network Policy may result in discipline up to, and including, suspension or termination. Employees that report violations, or suspected violations of CDC policy will be protected from termination, discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined. *(Refer also to student discipline policy # 5050C)*

If you identify computer security vulnerability, you are required to report it immediately.

h. Termination of Employment and/or Student Suspension

All information on user computers is considered CDC property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination requires administration authorization. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the CDC to continue using the computer, and information, uninterrupted.

The following activity is prohibited upon termination, and will be prosecuted to the fullest extent of the law:

10. Accessing CDC computers
11. Providing third parties, or anyone else, access to CDC computers
12. Taking computer files, data, programs, or computer equipment

V.Privacy

a. Monitoring Computer Communications and Systems

Many people think data stored on computers, transmission of data between individuals on dial-up modem lines, communications on the Internet, and e-mail are private, and in most cases they are. However, the CDC reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information, and will do so for legitimate purposes.

Random audits to verify that CDC computers are clear of viruses, and used in accordance with CDC policy, may be performed. The Technology Services Department will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The Technology Services Department will monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged. Again, computer systems and information are CDC property, and should be used principally for educational purposes.

The CDC reserves the right to block any web site it deems inappropriate using filtering technology. This may include but is not limited to sites that portray pornographic images, illegal activities, hate or violent content. The CDC is under no obligation to unblock any previously blocked site for any reason.

It is not the administration's intention to be "Big Brother." However, it is administration's fiduciary responsibility to:

13. Establish and enforce policy to help prevent the violation of personal rights and illegal acts
14. Reduce the risk of liability

15. Maintain a professional work environment where computer abuse will not be tolerated

VI. External Communications

a. Third Parties

The same standards of decorum, respect, and professionalism that guide us in the educational environment apply to computer communications with third parties. Important, confidential, and proprietary information is stored on CDC computer systems. Accordingly, only CDC personnel are allowed access to the school computer systems that contain confidential information, without written authorization from administration. Administration must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate need, duty, legal right, or obligation to access, disclose, or use information transmitted.

b. Dangers of the Internet

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Hackers exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

c. Internet Connections

Internet connections are authorized for specific educational needs only. Physical connection to the Internet without administration authorization is prohibited. Furthermore, the following activities are prohibited without administration authorization:

16. Accessing the Internet by circumventing an installed firewall
17. Downloading information of any kind, that is not intended for educational purposes, including web pages, data, files, programs, pictures, screen savers, and attachments
18. Research for personal business purposes
19. Copying programs
20. Transmitting important, confidential, or proprietary information
21. Speaking on behalf of the CDC

Individuals that have received administration approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the CDC. Disclaimers such as "***The opinions expressed do not necessarily represent those of the company,***" while a good idea, do not necessarily relieve the company of liability. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent record, and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

22. Portraying yourself as someone other than who you are, or the school you represent
23. Accessing inappropriate web sites, data, pictures, jokes, files, and games
24. Inappropriate chatting (chatting is only authorized for educational activities that are closely monitored by the teacher)
25. Inappropriate e-mail, monitoring, or viewing
26. Harassing, discriminating, or in any way making defamatory comments
27. Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
28. Gambling or any other activity that is illegal, violates CDC policy, or is contrary to the CDC's interests
29. Accessing sites for personal business gains, such as, stock investments, online auction services, and business solicitations.

d. Telephone and Fax Use

Authorization from administration is required before making any long distance phone calls or faxes.

Employees and/or students are prohibited from using CDC telephones to make personal long distance calls or faxes. Authorization from administration may be granted in case of an emergency. (Subject to any stipulations assigned by administration.)

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of telephone and fax.

VII.Email

a. Electronic Communications

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of education. It makes dissemination of information easy and cost-effective. Please take full advantage of it.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail.

Incidental or occasional use of e-mail for personal reasons is permitted. However, only CDC personnel are allowed access to the e-mail system. The following e-mail activity is prohibited:

30. Accessing, or trying to access, another user's e-mail account
31. Obtaining, or distributing, another user's e-mail account
32. Using e-mail to harass, discriminate, or make defamatory comments
33. Using e-mail to make off-color jokes, or send inappropriate e-mail to third parties

34. Transmitting records within, or outside, the CDC without authorization
35. Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes

Employees are required to report inappropriate use of e-mail.

Appropriate e-mail etiquette is essential to maintaining a productive and professional work environment. Comments that might be made at parties, in elevators, and on the telephone are now done via e-mail. However, e-mail does not disappear into thin air. It can be widely, easily, and quickly disseminated. E-mail can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. For professionals with electronic recovery skills, e-mail is a gold mine. If you would not put it in a memorandum on CDC letterhead, do not say it with e-mail!

b. Spam

Sending unsolicited messages or files to individuals, groups or organizations that you do not have a prior relationship with is prohibited, without written authorization from your supervisor. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of CDC policy and will be prosecuted to the full extent of the law.

VIII. Local Area Network

All important, confidential, or proprietary information must be stored on the LAN. Storing information of this type on your desktop computer is prohibited, without authorization from administration. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and back up are performed on the LAN; and programs and other information are updated regularly. Use the LAN! It is safe, effective, and reliable. Because important, confidential, and proprietary information is stored on the LAN, only CDC employees are allowed access, without written authorization from administration. All CDC policies apply to the LAN. The following activities are prohibited, without administration authorization:

36. Installation of business or personal software on the LAN
37. Making any changes to the LAN hardware or software
38. Accessing without authorization, or exceeding authorization, LAN programs, data, and files
39. Assisting anyone within, or outside, the CDC in obtaining access to the LAN

Glossary of Terms

Computer Information Data, software, files, and any other information stored on CDC computers and systems.

Encryption The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Hacker (Slang) an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Hot Links A connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in another.

Intranet A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents.

Internet The mother of all networks. A group of networks connected via routers.

ISDN Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services, and are much faster than the highest speed modems.

LAN A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Login A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

RAM Random Access Memory. The working memory of the computer. RAM is the memory used for storing data temporarily while working on it, running applications programs, etc. "Random Access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server A computer or device that administers network functions and applications.

Spam Unsolicited email often in the form of commercial announcements and may be referred to as electronic junk mail.

Trojan horse A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus A set of instructions that can reside in software; and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm A program that propagates by replicating itself on each host in a network, with the purpose of breaking into systems.