Manual of Policy and Procedures

Title	Number	Page
COMPUTING AND TELECOMMUNICATIONS TECHNOLOGY CONDITIONS OF USE POLICY	502	1 of 4
	Date 3/18/2010	

Network capacity is finite. Because of this, the VSC retains the right to manage the availability of network resources, in accordance with the following priorities:

HIGHEST:	All education, research, and administrative purposes of Vermont State Colleges.
MEDIUM:	Other uses indirectly related to Vermont State Colleges' purposes with education or research benefit, including personal communications.
LOWEST:	Recreation and entertainment.
NOT PERMITTED:	Any use that is a violation of the VSC Rules for the Use of Computing and Telecommunications Technology.

II. AUTHORIZED ACCESS WITHOUT NOTICE TO THE USER

A. VSC staff shall have access to a VSCnet user's resources to perform the following tasks without notice to the user:

1) Diagnosis – tasks necessary to identify or diagnose and correct systems problems.
2) Maintenance – tasks necessary to the health of VSCnet, including backups, scans, and other essential business functions of the VSC.
3) Compliance with state or federal law including a lawfully issued subpoena, court order or other compulsory legal process.
4) To address a health or safety emergency.

Suspected violations of any VSC policy discovered during the performance of these tasks will be reported to the Chief Technology Officer. All other information accessed during such tasks will be treated as confidential, except as otherwise permitted or required by VSC policy or law.

B. Only the Chancellor, President, or designee may authorize any other tracking, monitoring, or accessing of VSCnet resources without notice to the user. Authorization for these activities shall be based on a reasonable belief that one or more of the Rules for the Use of Computing and Telecommunications Technology has been or is being violated, or is necessary to conduct college or system business.

III. COMPLIANCE

A. User Compliance

Violations of this Policy by students may lead to loss of VSCnet privileges and/or discipline up to and including dismissal. Violations of this Policy by employees may lead to loss of VSCnet privileges and/or discipline up to and including termination. Any employee disciplinary action considered in association with this policy shall follow procedures set forth in the relevant employee collective bargaining agreement or, in the case of employees not covered by a collective bargaining agreement, the VSC Personnel Handbook. Students and employees who engage in activity related to copyright infringement may be liable for civil and/or criminal penalties.

B. Institutional Compliance with the Higher Education Opportunity Act

1. Each college shall provide an annual notice to students:
   a. notifying students that violations of federal copyright laws may subject them to civil and/or criminal penalties, including a summary of the penalties for violating federal copyright laws.
   b. describing the VSC policies related to unauthorized peer-to-peer file sharing, including disciplinary actions that may be taken against students who engage in unauthorized distribution of copyrighted material using the VSCnet.
2. The VSC shall maintain a plan, approved by the Chancellor, to effectively combat the unauthorized distribution of copyrighted material.

IV. RULES FOR THE USE OF VSC COMPUTING AND TELECOMMUNICATIONS TECHNOLOGY

1. VSCnet may not be used to violate any VSC policy or for threatening, obscene, harassing and or libelous conduct.
2. VSCnetmay not be used for illegal purposes under local, state or federal law including copyright violation, libel, criminal threatening, fraud, etc.
3. VSCnet may not be used to send unsolicited advertising, to propagate computer worms and viruses or for computer hacking within VSCnet or on the Internet.
4. Sharing one's password with others and allowing others to use one's password or user identity or address are prohibited, unless specifically approved by the Chancellor, the appropriate college President, or designee.
5. Using a password other than one's own is prohibited, unless specifically approved by the Chancellor, the appropriate college President, or designee.
6. Unauthorized access to any information or data on VSCnet is prohibited.

7. Tampering with the physical network (cables, hubs, computers and peripherals etc.) is prohibited.
8. Intercepting or attempting to intercept data is prohibited.
9.