VSC
VERMONT STATE COLLEGES

Manual of Policy and Procedures

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

I. PURPOSE

The purpose of this policy is to define permissible behavior of those Vermont State Colleges ("VSC") employees, students and others using VSC computing and telecommunications resources ("VSCnet) in order to preserve the confidentiality, availability, and integrity of VSCnet resources and promote the goals and values of the VSC.

The Vermont State Colleges (VSC) owns and maintains computing and telecommunications technologies to support the education, research and daily work of its faculty, staff, and students. This policy applies to any user of VSCnet resources. The right to use VSCnet, its resources, and the Internet is dependent upon compliance with this policy.

By connecting thousands of computers at the Vermont State Colleges with each other and with national and international networks, VSCnet provides a wide range of educational benefits. The VSC values freedom of expression, scholarly inquiry and information sharing provided they are consistent with VSC policies, and state and federal laws and constitutional provisions.

Concomitant with these values is the personal and professional obligation of each member of our community to use computer and network resources responsibly, ethically, and in accordance with the laws and rights of others. The use of shared resources relies on a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

Nothing herein shall be construed to preclude authorized information technology staff from performing their work including diagnosis, compliance with law, maintenance tasks, and the support of investigations instituted pursuant to the procedures set forth in this Policy. The VSC will seek to maintain system security and privacy, but the VSCnet exists for the furtherance of VSC business and users should not have an expectation that information in user accounts, or on VSC-owned or –administered computers, is private.

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. VSCnet may 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. Originating or attempting to originate email from someone else is prohibited.
10. Logging on or attempting to log on to any piece of VSC computer equipment without an account is prohibited.
11. Using or attempting to use any network address or identity one has not be assigned by VSC or college authorities—even on a machine one may own—is prohibited.
12. VSCnet may not be used for profit-making activities.
13. Selling network access is prohibited.
14. Unreasonable or inappropriate use of VSCnet and computing resources for personal business is prohibited as is using more than a fair share of such resources.
15. Publishing or otherwise making available on a web, ftp, file or other server any information, software, document, graphic or icon without permission of the copyright owner is prohibited. This includes sharing downloaded music and video without permission of the copyright owner.
16. Attempts to deny VSCnet access to others via mail bombs, chain email, spam and similar automated processes is prohibited.
17. VSCnet users are prohibited from granting access to VSCnet resources (for example, computers, services, or data) to persons not associated with the Vermont State Colleges or to persons associated with the Vermont State Colleges who have been denied network access
18. The installation and/or removal of any software on a VSC- or college-owned machine without the specific written permission of the Chief Technology Officer (CTO), unless authorized by college policy or procedures, is prohibited.
19. The installation of any hardware device or component on a VSC or college-owned machine or the removal of such a device or component from a VSC or college-owned machine without the specific written permission of the CTO, unless authorized by college policy or procedures,. is prohibited.
20. Connecting a computer to VSCnet without specific written permission of the CTO, unless authorized by college policy or procedures, is prohibited.
21. Operating a server of any kind on VSCnet without specific written permission of the CTO is prohibited. Operators of approved servers must provide server passwords to the CTO on demand.
22. Registering a domain name associated with a VSC IP address without specific written permission of the CTO is prohibited.
23. Other use of VSCnet resources for purposes inconsistent with the mission of the VSC and the purposes set forth above is prohibited.

Signed by:	Timothy J. Donovan Chancellor