1.0 Purpose

This document identifies the rights and responsibilities of those who use the electronic information resources at Saint Michael's College. This includes the use of academic and administrative computer systems, the networks, the on-campus information resources including telecommunications systems, and the Internet resources reached through Saint Michael's College systems.

2.0 Scope

This policy applies to all users of all information systems that are the property of Saint Michael's College. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by Saint Michael's College.
- All contractors and third parties that work on behalf of and are paid directly by Saint Michael's College.
- All contractors and third parties that work on behalf of Saint Michael's College but are paid directly by an alternate employer.
- All employees of partners and clients of Saint Michael's College that access Saint Michael's College's non-public information systems.
- All students, graduate and undergraduate, whether enrolled full time or part-time at Saint Michael's College.
- All guests of the College.

3.0 Policy

3.1 Rights and Responsibilities

The College makes technical resources, including, but not limited to, computer accounts, electronic mail services, Internet access, and telephone service, available to staff and faculty for academic and administrative purposes. These resources may be used only by you or by the employee (including work study students) to whom you have delegated responsibility for that resource. You may only delegate authority for an account to someone else with the permission of the Department of Information Technology. If you delegate responsibility for a particular resource to someone else, you are still responsible for its appropriate use.

The electronic information systems at Saint Michael's College are provided for the purposes of instruction, research, personal development, and administration. The College has developed policies and procedures to insure the systems are used for their intended purpose. Users have the responsibility to abide by these policies but also should have the expectation that the systems will be administered to the extent possible in a manner consistent with the College's educational mission. This policy applies to all users of Saint Michael's system resources, including those who access these resources from off campus.

The College seeks to provide an environment in which academic usage has the first priority, and in which there is respect for freedom of inquiry and expression; opposition to censorship; privacy and confidentiality; freedom from sexual and other unlawful harassment; and protection of intellectual property. The same standards and principles of intellectual and academic freedom already supported by the College in other areas extend to material received and sent through the network. Furthermore, the same standards of intellectual and academic freedom developed for faculty and student publication in traditional media are also applicable to publication in electronic media.
In addition, respect for law, for due process, and the presumption of innocence are crucial elements of this environment.

Users are expected to abide by the policies of the College, whose existence makes the use of these resources available. Every user is also expected to be considerate of the rights of other users.

3.2 Privacy and Security

Network and system administrators are expected to treat the contents of electronic files as confidential, except to the limited extent necessary to inform appropriate College officials of potential violations of these or other College policies or laws. However, normal operation and maintenance of the systems requires backup and caching of data and communications, the logging of activity, and the monitoring of general usage patterns. In particular, users should be aware that systems administrators may examine files as part of these activities. Users should also know that public lab computers have no private, secure storage and work should not be kept there.
In all matters relating to privacy and security of communications and individual accounts as well as requests for release of information, College personnel will abide by any applicable U.S. law, Vermont laws and/or College policy. Records may be examined or disclosed, for example, in response to a proper subpoena or court order from external attorneys, police, and/or administrative agencies, and in response to on-campus investigations following College Security procedures, or investigations of suspected

violations of these or other College policies or laws. Employees should take all necessary steps to prevent unauthorized access to confidential information. Examples of confidential information include but are not limited to: company sensitive, financial data, customer lists, research data, and student, faculty, staff and alumni lists containing identifying information.

Authorized users are responsible for the security of their passwords and accounts. In order to prevent the compromise of an account, all computers should be locked, or turned off, when unattended. The Password Standard and Computer Security Standard documents outline the rules and guidelines for securing passwords and accounts.

Users shall not open any e-mail attachment received from unknown senders, or any email attachment that is unexpected, even if the sender is familiar. Such attachments may contain viruses, e-mail bombs, or Trojan horse code. Suspicious email messages should be forwarded to ithelp@smcvt.edu for review.

All devices that are connected to the College's Network/Internet/Intranet/Extranet, whether owned by the College or the individual, shall be continually executing approved virus/Ad-Ware scanning software with a current virus database unless overridden by departmental or group policy. The Computer Security Standard provides information on best practices, as well as, the full list of approved anti-virus software.

- Personal devices connecting to the College network must be registered and scanned for compliance through network access control systems.
- In order to pass the scan, all computers must have approved antivirus software installed, have up-to-date antivirus signatures and have up-to-date operating system patches installed.

3.3 General Use & Ownership

You must abide by all other College policies and procedures and may not use these resources to violate those policies. For example you may not knowingly use these resources to compose, transmit, access, print, or download content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any staff, faculty member, or other person. Data inquiries or information searches not directly related to your job responsibilities may also result in disciplinary action. Furthermore, you must follow College policies established to ensure efficient and secure operation of the system; for example, policies to protect system resources from viruses.

Use of the College's technical resources is subject to monitoring for security, network management, or other management purposes. Monitoring may include accessing recorded messages and printing or reading data files or entering offices to examine records and files electronic or printed. Monitoring may also include review of files recording your Internet use, and auditing of all firewalls.

College technical resources are to be used for College business with each administrative area assuming responsibility for its use. Limited personal use of these resources is permissible. The College may seek reimbursement from you for costs of personal use of any of these resources. When possible violations of this policy threaten the integrity or security of the network or other technology resources, the Information Technology staff may act to prevent or repair any such problem without prior notification to, or consent of, any user. Those actions may include suspending the privilege to use the resources in question.

Your use of the College's technical resources, including but not limited to, the College's e-mail and/or the Internet or Intranet, telephone, or computer account constitutes your consent to review by the College. If you use the systems, you agree to use them according to the rules and the College reserves the right to enforce those rules in any way it deems necessary.

3.4 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College or the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an IT Asset to actively engage in procuring or transmitting material that is in violation of any law or that could create a hostile work environment.
- Providing information about, or lists of, SMC employees to parties outside the College.
- Circumventing user authentication or security of any IT asset.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, network sniffing, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Port scanning or security scanning is expressly prohibited unless prior notification to Saint Michael's College is made or is within the employee's regular job duties. Executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is part of the employee's normal job/duty.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet, whether inside or outside the College's network.
- Using the Saint Michael's College system for illegal or criminal purposes.
- Unauthorized use of resources for commercial enterprises.
- Providing confidential and/or personal information regarding any person or entity to parties outside the College, including SMC ID numbers, Social Security Numbers, home addresses, personal telephone numbers, credit card numbers, etc.
- Substantially and willfully interfering with another person's authorized use.
- Compromising or attempting to compromise privacy or confidentiality. In particular, attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness.
- Modifying or attempting to modify system facilities without authorization, including software or hardware installation. This includes the use of the Saint Michael's College system as a staging ground to crack other systems.
- Obstructing other people's work by consuming gratuitously large amounts of system resource (e.g., network bandwidth or printers). This includes, but is not limited to, game playing or monopolizing information resources for entertainment or personal use.

- Abuse of printing privileges, including printing of excessive copies or in violation of copyright.
- Violating license agreements.

4.0 Standards and Guidelines

- Standard for Computer Security
- Personnel Security Guidelines
- Peer to Peer File Sharing Guidelines

5.0 Enforcement

Violation of any of the constraints of this policy or procedures may be subject to discipline as outlined in the employee and student handbooks, or a termination of the contract in the case of contractors or consultants. Additionally, individuals may be subject to loss of Saint Michael's College information resource access privileges, may be subject to legal action, and may also be held financially liable.

The College reserves the right to revoke access privileges at its sole discretion in the event of a threat to network security or a security breach.

Notification of possible violations may be made to the Helpdesk at 802.654.2020 or to abuse@smcvt.edu.