1.0 Purpose

The purpose of this policy is to outline the responsibility of the Information Technology Department staff and user rights with respect to the privacy of electronic files and communications stored on the Saint Michael's College network and institutionally-owned computers and mobile devices.

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.

3.0 Definitions

3.1 Personally Identifiable Information (PII): "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information," as defined by the National Institute of Standards and Technology (NIST).

3.2 Users: Users includes all members of the Saint Michael's College community to the extent they have authorized access to College data, and may include students, faculty, staff, contractors, consultants and temporary employees and volunteers.

4.0 Policy

4.1 Information Technology Department Staff Roles and Responsibilities

- The College will typically review electronic files and communications of our end-users only when there is a reasonable system security or management activity basis for doing so. Network and system administrators are expected to treat the contents of electronic files as confidential, except to the extent necessary to inform appropriate College officials of potential violations of this or other College policies or laws and required to monitor system security and performance.
- Network and system administrators will perform targeted searches at the direction of the Vice President of Human Resources and Administrative Services, the Chief Information Officer and a relevant area Vice President. All three must agree to the search. When a search targeting a specific individual has been authorized the subject of the search will be notified when in the judgment of those who authorized the search determine it is practical to do so.
- 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 Internet use, and auditing of all firewalls. In particular, users should be aware that systems administrators may examine files as part of these activities.
- 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 this or other College policies or laws.
- The personnel charged with the administration of the College's computing systems and file servers take their obligations to protect individuals' privacy seriously. In accordance with general College policy, inappropriate use, access, or sharing of confidential information may expose the individual to College disciplinary action.
- The College will take reasonable steps to protect personally identifiable information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. The College has implemented appropriate physical, electronic, and managerial processes to secure private information from loss, misuse, unauthorized access or disclosure, alteration, or destruction. We cannot guarantee the security of personally identifiable information on or transmitted via third-party electronic networks such as the Internet.

4.2 User Rights and Responsibilities

- Unless otherwise notified by the collecting office, information provided to the College may be shared among offices within the College and outside entities as necessary or appropriate in the conduct of legitimate college business and consistent with applicable law.
- Users may inspect and/or correct electronic information that has been collected about them.
- Institutionally-generated, personally identifiable information must not be stored on college-owned or personally-owned devices.
- By its very nature email is not a secure or confidential form of communication. Sensitive or personally identifiable information should not be sent through email.
- As a matter of principle and ethics, individuals bear the responsibility for assuring that e-mail messages, including attachments and previous appended messages, are forwarded only to parties whose interest is consistent with the purpose of and intent of the previous correspondents. If in doubt, obtain the consent of the original correspondents before forwarding.
- College computing resources are provided for educational and administrative purposes. We recognize that computing resources will be used for storing and communicating many types of information, including that of a personal nature. Members of the College community are expected to be judicious in their use of computing resources and understand that the College is obligated to inspect these systems for sensitive and malicious content. 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 acknowledgement of potential 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.

5.0 Related Policies

5.1 Information Technology Appropriate Use Policy

5.2 Data Security Policy

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