| | |
|---|---|
| **Name:** | **Policy on Information Technology** |
| **Policy Number:** | 2-2004 |
| **Approving Authority:** | President |
| **Approved:** | September 2000 |
| **Responsible Office:** | Enterprise Information Technology (EIT) |
| **Responsibility:** | Chief Information Officer |
| **Revision Dates:** | November 4, 2021, May 2012, November 2006 |
| **Supersedes:** | Policy on Email, Intranet/Internet & Voice Mail (September 2000) |
| | Policy on Computer Ethics and Computer Abuse |
| **Next required review:** | November 2024 |

---

## 1. Preamble

Saint Mary's University owns or leases all University information technology (IT) which is made available to faculty in support of their teaching, research, and administrative activities; to staff in support of their assigned responsibilities; to students in support of their academic objectives and requirements; and to other authorized users.

Information Technology includes, but is not limited to, Email, Intranet, Internet, Voice Mail systems, databases, computers and associated peripherals, mobile devices, the telecommunications infrastructure and related equipment, and all software accessed through Saint Mary's networks.

## 2. Purpose

The purpose of this policy is to establish the responsibilities of the University community with respect to their use of Information Technology (IT) resources, and those actions necessary or that should be avoided in order to fulfill these responsibilities.

## 3. Scope/Jurisdiction

This policy applies to all university faculty, staff, and students, and to others who are authorized users of Saint Mary's University information technology, whether on campus or remotely.

The application of this policy will not be inconsistent with relevant collective agreements.

## 4. Policy

**4.1 Policy Statement.** The use of Saint Mary's University information technology (IT) resources must be consistent with the academic mission of the University. These IT resources are provided to support the teaching, learning, research, and administrative activities of the University community. Users of University IT may have access to valuable internal and external networks and resources, and confidential information, and all users are expected to use these resources in a responsible, ethical, and legal manner. User actions should not

adversely affect the ability of others to use these resources or compromise the security and privacy of information.

**4.2 Responsibilities:**

- **Users of university IT resources shall use University IT resources for the academic and administrative purposes for which they are intended. Users will:**

a. Use only those IT resources that they have been authorized to use, unless those resources are intended to be generally available to the University community; and

b. Not use IT resources for commercial activities unless such activities have been authorized in writing by the University, and do not adversely impact other users, or introduce risk to the security of personal or confidential information or the University IT infrastructure.

c. Limit personal use of University IT to modest, infrequent purposes. University IT facilities should be used primarily for university related educational and administrative purposes.

- **Users will not adversely affect the ability of others to use IT resources within or external to the University or compromise the integrity or reliability of those IT resources. Users will:**

a. Adhere to the rules governing use of accounts, equipment, networks, or other facilities and to licensing agreements entered by the University.

b. Not use IT resources in a manner that interferes with the normal operation of IT resources within or external to the University or hinders or encroaches on the ability of others to use those resource.

- **Users will not compromise the security and privacy of sensitive information. Users will:**

a. keep user authentication credentials, such as user accounts and passwords or similar authentication credentials, secure, such that they cannot be used by others;

b. choose secure passwords for their user accounts;

c. preserve the confidentiality of any University information to which they have access in the course of employment or academic activities at the University;

d. preserve the privacy of any personal or confidential information about or belonging to other individuals, to which they have access in the course of employment or academic activities; and

e. take the necessary precautions to prevent theft or unauthorized use of computers, storage devices, and information.

- **Users will use IT resources in a manner which is consistent with all University policies and does not cause damage to the University. Users will:**

a. maintain familiarity with University policies, and seek clarification from EIT about any elements that are unclear; and

b. adhere to the terms of any contractual agreements or arrangements between the University and external service providers or organizations and use such resources for the intended academic and/or administrative purposes only.

- **Users will not violate the rights of others or contravene the laws of Canada and/or the Province of Nova Scotia in their use of IT resources. Users will:**

    a. respect the copyright and intellectual property rights of others, whether at the University or elsewhere;

b. respect the licensing agreements and terms for all software, and only install and use software as permitted in the license agreement for that software

c. respect the licensing agreements and terms for all electronic resources including databases, journals, books and other print, audio, and video content

d. not use University IT resources for any activities or actions which are illegal or do not comply with Canadian or Nova Scotia legislation; and

e. not use University IT Resources to do anything that is a violation of the rights of others, such as displaying or distributing obscene, harassing, defamatory, or discriminatory material or messages.

f. Not use University IT for any purpose that is malicious, unethical, interferes with University activities and functions or does not respect the image and reputation of Saint Mary's University.

## 5. Usernames and Passwords

Access to IT systems is gained via a username and a password. Such access is generally referred to as an account. Application for account access may be obtained from the EIT Help Desk or on the SMU website.

All accounts are granted to individuals; they are not to be shared with friends, family or others. The owner of an account is responsible for all use of that account.

A password is secret; it should be known only by the account owner.

Account owners are required to change their password when prompted by the system.

## 6. Privacy

Saint Mary's University attempts to provide secure IT services; however, the security and confidentiality of these systems cannot be guaranteed.

Users should not have any expectation that their Email, Voice Mail or Intranet/Internet communications are private. Assigning confidential passwords or using email "sensitivity" settings does not mean that the use of information technology is private or secure. All personal data stored on University owned computing devices should be viewed as insecure, and not private.

The University reserves the right to monitor and access user accounts, and data stored on University owned IT computing resources, in order to conduct its business in a secure and reasonable manner. Only authorized personnel in the performance of their employment duties may access and monitor the use of information technology.

The University will treat data as confidential and will not examine or disclose information without just cause nor disclose information to a third party unless it is for use in a disciplinary or criminal investigation or has been the subject of a subpoena served on a representative of the University. Authorizations to access, search, or disclose personal data will require the approval of the Vice President, Finance & Administration, or the Senior Director, Legal Services.

The University is bound by the requirements of Freedom of Information / Protection of Privacy (FOIPOP) legislation.

## 7. Abuse

It is contrary to University Policies to interfere with or disrupt network users, services, or equipment. This includes all conduct that is contrary to Section 4.2 above, and also includes:

- Unauthorized access, alteration, destruction and removal of information, equipment, software or systems.
- Using or attempting to use another person's account/password.
- Tampering with another user's account, email, web pages, or voice mail
- Disclosure of confidential passwords, data, information, or access devices to anyone other than authorized University personnel.
- Attempting to bypass standard procedures. This includes, but is not limited to: refusal to display correct identification, unauthorized use of a password, accessing a file without permission, and reading an executable only file.
- Using University systems for distributing chain mail; sending forged or anonymous e-mail or postings; and viewing, sending, or printing offensive material.
- Maintaining and using an account after withdrawal from the course for which the account was assigned.
- The collection, copying and use of computer output, other than the User's own, without the owner's permission.
- Breaking regulations applicable to the discussion groups, bulletin boards, databases, and computer systems available through the Internet.
- Using IT systems for political activities

## 8. Policy Violations

Saint Mary's University considers any violation of this policy to be a serious offence. Failure to comply with this policy may result in fines, access privileges being revoked or restricted and disciplinary action up to and including dismissal depending on the severity and nature of the act. In some circumstances, individuals may also be liable for civil and criminal prosecution.

Complaints against students will be handled by the Associate Vice President, Student Affairs and Services. Complaints against faculty will be handled by the appropriate Dean. Complaints against staff will be handled by the appropriate Department Head. Complaints will be investigated with assistance of EIT.

The University may put technologies in place to automatically enforce policies, protect IT resources, and preserve the University reputation.

## 9. Relevant Legislation

- Freedom of Information and Protection of Privacy Act (Nova Scotia).
- Personal Information International Disclosure Protection Act (Nova Scotia)
- Personal Health Information Act (Nova Scotia)

## 10. Related Policies, Procedures & Documents

10.1 The following policies are related to this Policy and should be referred to as required for interpretation or understanding:

a. Privacy Policy (12-003)