SAINT MARY'S UNIVERSITY SINCE 1802

One University. One World. Yours.

Name:	**Policy on Information Technology**
Policy Number:	2-2004
Origin:	Information Technology Systems & Support (ITSS)
Approved:	September 2000
Issuing Authority:	Vice President, Administration
Responsibility:	Director, Information Technology Systems & Support
Revision Dates:	November, 2006, May 2012
Effective Date	22 May 2012
Supersedes:	Policy on Email, Intranet/Internet & Voice Mail (September 2000) Policy on Computer Ethics and Computer Abuse

1. Introduction

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 assure that the Saint Mary's University community is informed about the use of and access to IT systems.

3. Scope

This policy applies to all users of Saint Mary's University information technology

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

4. Responsibilities

<u>ITSS:</u>

- ITSS is responsible for the maintenance and management of all central IT resources.
- ITSS provides creation, management, and distribution of Saint Mary's University IT

Accounts.

Users:

- Users must adhere to the rules governing use of accounts, equipment, networks or other facilities and to licensing agreements entered into by the University.
- Adherence to provincial or federal laws and University policies is required.
- Users must respect the rights and property of others and consider other persons using shared systems and equipment.
- Although modest personal use of University Information Technology is allowed, University IT facilities should be used primarily for University related educational and administrative purposes.
- Any use of University Information Technology that is malicious, unethical, interferes with University activities and functions or does not respect the image and reputation of Saint Mary's University is not permitted.
- Unless authorized to do so, users must not use University systems to give the impression that they represent the University.

5. Systems Access

Saint Mary's University provides information technology for legitimate University-related activities to faculty, students, staff, and other individuals and entities granted IT privileges at Saint Mary's University.

Information Technology use is subject to the normal requirements of legal and ethical behaviour within the University community and does not extend to whatever is technically possible.

6. 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 ITSS 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 by only you. Anyone who knows both your username and password will be able to access your IT account. You will be held accountable for any abuses carried out via your account.

To prevent abuses being carried out it is strongly recommended that you:

- Do not tell anyone your password.
- Do not write down your password.
- Do not use a simple word as a password.
- Do not use personal information as a password.
- Do not reuse an old password.
- Use a phrase as a password.
- Use numbers and special characters in a password.
- Change your password every 90 days.

ITSS may adopt technology to support these practices and to provide a secure environment.

7. Privacy

Saint Mary’s University attempts to provide secure IT services. Operators of University IT systems are expected to follow sound professional practices in providing for the security of electronic communications, data, information and records under their jurisdiction. Since such professional practices and protections are not foolproof, 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, Administration.

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

8. Abuse

It is contrary to University Policies to interfere with or disrupt network users, services or equipment. This includes, but is not limited to:

General:

- Unauthorized access, alteration, destruction and removal of information, equipment, software or systems.
- Using or attempting to use another person’s account/password. Users who reveal or allow others to use their accounts may find themselves restricted if others abuse the system using their account.
- 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.
- Use of Saint Mary’s University computer equipment or software to violate the terms of any Software License Agreement.
- 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 the services in a malicious, threatening, or obscene manner; or to harass others.
- Using University systems and resources for commercial purposes outside University business activity; or for personal financial gain.

- Using University systems for distributing chain mail; sending forged or anonymous e-mail or postings; and viewing, sending, or printing pornographic material.
- Maintaining and using an account after you have withdrawn from the course for which the account was assigned.
- The collection, copying and use of computer output, other than your 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

Computer labs:

- Using computer labs for anything but coursework when the labs are more than 70% full.
- Tampering with a workstation. (Please report all broken equipment and software to the ITSS Help Desk, Local 8111.)
- Using more than one lab workstation at a time.
- Disrupting computer labs with noisy behaviour, offensive language, or making a mess.
- Refusing to leave a computer lab when requested by the Instructor, Lab Assistant, or Security.

9. 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 Director of Student 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 ITSS.

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