3.E-2002 Statement on Use of St. Mary's University Computing and Network Resources

1. Overview

Computing and network resources are important components of the University infrastructure. This statement provides guidelines that govern the appropriate and ethical use of these resources, informs users of expectations and responsibilities assumed in the use of St. Mary's University (University) computing and network resources, and clarifies the context.

2. Guiding Principles

2.1 The University encourages the use of computing and network resources to enhance the working and learning environment of its members.

2.2 These resources are provided primarily to support and further the mission of the University.

2.3 The University values and strives to provide its members with an environment of free inquiry and expression. Freedom of expression and academic freedom should be limited to no greater degree in electronic format than in printed or oral communication.

2.4 Members of the University community are responsible and accountable for their actions and statements, which includes showing reasonable restraint in the consumption of shared resources. There is an expectation of appropriate and ethical behaviour in the use of computing and network resources. Users of computing and network resources are expected to comply with applicable provincial and federal laws and pertinent University policies and procedures.[1]

2.5 There is a presumption of privacy. The privacy of system users should be respected and reasonable safeguards in place to protect it.

Approval Authority	Responsible Office	Effective Date	Date Last Revisited	Review Frequency
President's Council	Finance	September 2002		Every 5 years

3. Rights/Responsibilities

Contained within and following from the Guiding Principles are a variety of rights and responsibilities of both the user and the University.

4. University Rights and Responsibilities

4.1 To allocate the use of and access to university computing and network resources.

4.2 To define access privileges of university users and, where just cause is present, to revoke access privileges of any University user.

4.3 To inform University users of their rights and responsibilities in the use of university computing and network resources, and to commute clearly the terms and conditions under which access to and use of such resources are provided.

4.4 To ensure reasonable safeguards are in place to protect the privacy of university users.

4.5 To ensure reasonable security for university computing and network resources, and where just cause is present, to act upon complaints in a reasonable manner.

5. User Rights and Responsibilities

5.1 To a presumption of privacy in the use of the computing resources assigned. Users should keep in mind that certain information is gathered routinely for administrative purposes.

5.2 To use University computing and network resources in a manner which does not unduly interfere with the study, work or working environment of other users.

5.3 To be accountable for the use of any computing and network resources assigned to the user.

5.4 To seek permission from the appropriate University authority to use University computing or network resources for fundamentally different purposes than those for which they were allocated.

6. University Rights and Responsibilities

6.1 Adjudication/Disciplinary Action

Misuse of the University's computing and network resources may result in disciplinary action within the University. Any such action undertaken will be governed by relevant University policies and procedures.[2]

Appendix to Statement on Use of St. Mary's University Computing and Network Resources

1. **Interpretation/Examples**

   This appendix provides selected examples to assist in the application and interpretation of the Statement. While such examples may appear straightforward, there is often a fine balance in interpreting the principles that apply to the situation. One should be cautious about making decisions not supported by policy.

2. **Free Inquiry and Expression**

   The following example describes inappropriate responses to situations based on the guiding principle concerning freedom of expression and academic freedom (especially as it pertains to electronic formats being limited to no greater extent than a printed or oral communication). In all cases, even those in which the material may be deemed offensive, the appropriate University policy should be consulted.

   The student newspaper publishes both electronic and printed versions. An article is published in both that many individuals find offensive. The electronic version is ordered removed from the campus network, but no restriction is placed on the printed version.

3. **Privacy**

   Access to an individual's account should not be made without the informed consent of the individual.

   An individual no longer at the University has left data on a university computer, and another University researcher would like to access that data. The researcher asks the administrator of the system to transfer the data to his account.

   The following examples represent not only a violation of an individual's privacy, but also could result in criminal charges.

   A system administrator uses their privileges to read electronic mail stored on a friend's account without permission.

   A user obtains, or tries to obtain, covert or illicit access to another person's account (e.g., stealing or attempting to crack another person's password).

   The following examples describe circumstances where the actions are quite appropriate and do not constitute a violation of a user's presumption of privacy.

The manager of a system notices that a program run by a user has "run away," causing the disk to become full, thereby impeding the computing access of others. The manager terminates the program and deletes some of the newly generated files in order to regain adequate space. The manager informs the user of their actions and the reasons for them.

Local police are seeking evidence against a user and they serve the University with a valid search warrant. Only that information specified in the warrant is provided to the police and the owner of that information is advised of its disclosure.

Aware that breaches of security represent a significant problem, the administration authorizes the system administrator to run a program, which looks for suspicious filenames in users' file space. Files with suspicious names are investigated further.

A student in a public lab complains to the lab administrator that they are receiving harassing e-mails and has a reasonable idea as to their origin. The student requests that the administrator investigate immediately, before evidence can be destroyed.

4. Appropriate Use of Resources

The following example represents situations that are commensurate with the guiding principle concerning University's encouragement of the use of computing and network resources to enhance the working and learning environment of its members. In each of the examples, the assumption has been made that these activities are not specifically excluded in the definition of access privileges accorded the University user.

A user occasionally sends electronic mail to friends and/or relatives.

Normally, one should not share access to a computer account. This is particularly important for those with special access privileges and/or access to confidential information. However, if such access is provided, the owner of the account must assume supervisory responsibility and may be held accountable for the actions of others. With this understanding, the following example would also be seen to be an appropriate use of resources.

An individual allows a colleague visiting the University for the day to use their account to log in remotely to their computer.

Each of the following examples represents a violation of the guiding principle concerning the responsibility of users to be accountable for their actions and statements. In particular, no member of the University community (faculty, staff, student) should unduly interfere with the study, work or working environment of other members of the University.

A user refuses to consider alternatives when their web page (constructed on a computer) gets thousands of "hits" every hour, swamping the local network and impeding the access of other users.

During a time when many students require workstation access to complete their projects, a student locks a public workstation, then leaves for an extended period of time, thereby making the workstation unavailable to others.

A user posts a message to a newsgroup with a forged header, making it appear as though the message appeared from a second user.

A user plays very loud music on a workstation in a public terminal room, annoying other users.

A user distributes a chain letter or pyramid scheme through the campus network.

5. Violations of University Policy and/or the Law

The following examples are violations of university policy; as well, most are contrary to federal law. When such violations become apparent, they will normally in the first instance be dealt with according to university policies. Further action, as provided by statute, may also be taken. It is incumbent on users to be aware of university policies and relevant legislation.

A University user sends threats to another person via electronic mail.

A student somehow gains access to the University computer where course marks are stored, and surreptitiously improves their marks and those of their friends for several of their courses.

A professor buys one copy of copyrighted software, then makes 30 copies to distribute to students for use in their course, without payment to the copyright holder.

A user exploits a bug and thereby renders a computer unusable by others.

After a machine crashes, a system administrator discovers a hidden ftp site that is being used to distribute copyrighted software to many local users without the consent of the copyright holder.

A college user sells access to his computer account to a local business which wants to use it to gain cheap access to the Internet.

6. Harassment

The following examples constitute a violation of ethical behaviour, especially as it pertains to impeding the ability of others to study or work. Users should exercise discretion when printing, transmitting or displaying material.

After an argument, an individual uses e-mail to send repeatedly a very large file to the person with whom they argued. The effect on this person is that it restricts their ability to work on their system.

Mary tells John she does not want to receive any further e-mail communication from him, but John persists in sending messages.

A student in a lab displays images that are offensive in full view of others in the lab (ex: pornography, hate propaganda etc.). The student has been informed that some individuals in the lab find the images offensive and they are asked to stop displaying them. In spite of requests, the student continues to display the images.

A user sends a hate-mail message to all their class members.