ST. CLAIR COLLEGE
OF APPLIED ARTS & TECHNOLOGY

POLICY AND PROCEDURE MANUAL

Policy Title:	**ACCEPTABLE USE POLICY – COMPUTING, NETWORK & COMMUNICATION RESOURCES**	**Area of Responsibility: CHIEF INFORMATION OFFICER/ CORPORATE SECRETARY**
Policy Section:	**INFORMATION TECHNOLOGY**	
Effective Date:	**2005 01 01**	**Policy No: 6.2**
Supersedes:	**NEW POLICY**	**Page: 1 of 3**

6.2 Acceptable Use Policy – Computing, Network & Communication Resources

Coverage

This policy is applicable to the entire St. Clair College community using any device connected to the college network from any access point, internal or remote. This policy includes all privately owned computers connected to the St. Clair network. In this context, the college community includes: all registered students, both full-time and part-time; all paid employees, full-time, part-time and casual; all others associated with the college as such board members, retirees, or volunteers, and such visitors as are granted temporary user status by the college.

Introduction

St. Clair College encourages the use of computing and network resources to enhance the learning and working environment of the college community. However, access to the computing and network environment at St. Clair College is a privilege to be used in effective, ethical and lawful ways that support the values of the college. The college will endeavor to create an atmosphere that balances respect for individual computer users with respect for college facilities and college and community standards.

6.2.1 Principles

1. Computing and network resources are provided primarily to support and further the college mission.

2. College community users are expected to comply with provincial and federal laws and St. Clair College policies and procedures.

3. Members of the college community are responsible and accountable for their actions and statements in the electronic working and learning environment, according to the disciplinary policy of their respective jurisdiction.

4. Members are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.

5. Generally, with respect to computing accounts established for students, faculty and staff, there is a presumption of privacy. However, network administrators have access to all email, including data in transit and stored, and if an infraction is suspected, the traffic and files will be investigated in accordance with the applicable college policy.

6. In addition, college users accessing external networks are bound by their policies, and the more restrictive policy will apply.

6.2.2 Unacceptable Uses

Note: Unacceptable uses as outlined here are not limited to these examples

Unauthorized access (hacking): This may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security provisions of college or external systems.

Vandalism of data: Deliberate alteration or destruction of computer files is a Criminal Code offence (Section 430 [387]) and will be prosecuted. Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access.

Interference with other users' work: This includes use of any process that causes a user to be deprived of services or resources that they would normally expect to have available. It covers, but is not limited to the creation of "spam", and the introduction of viruses or chain letters.

Squandering resources: Resources are shared and no user may degrade the systems by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, unattended network connections and/or lengthy print jobs.

Sharing of account: The College's computing resources are allocated to groups and individuals for specific academic and administrative purposes. It is not acceptable to give, sell, or otherwise provide computing resources to individuals or groups that do not have explicit permission to use them from the college authority.

Commercial uses: The college system(s) may not be used to sell or promote products or services for personal gain. This includes uses such as distribution of advertising materials, the offering of network information or services for sale, and private enterprises. Faculty and staff are referred to the institution's policy on these matters.

Breach of copyright: This includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications or files without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed.

Offensive material: Materials not subject to legal sanction may be objectionable or repugnant to persons other than the computer user. Importation or distribution of such

material (including, but not limited to racist material, hate literature, sexist slurs or pornography) requires an underlying academic or educational purpose.

Hostile atmosphere: The display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content contravene the college's sexual harassment policy.

Harassment: Harassing or defamatory material may not be sent by electronic means, including email and voice mail, or posted to news groups.

6.2.3 Discipline, Jurisdiction and Penalties

Preamble: The College will not act as censor of information available on our campus network, but will investigate properly identified allegations arising within the member/users to ensure compliance with applicable federal and provincial laws and with college policies and procedures.

Adjudication/disciplinary action: Misuse of the college's computing and network resources may result in disciplinary action by the college. Violations of law will result in immediate loss of privileges and will be reported to the appropriate college and law enforcement authorities. Lesser violations by students will be dealt with under the Appeals, Complaints and Discipline Policy. Staff violations will be handled in accordance with the College's approved Progressive Discipline Procedure (found in the H.R. Handbook). In most instances of unacceptable behaviour or misconduct, disciplinary action progresses in steps from reprimand to discharge, consistent with the employee's prior disciplinary record and the flagrancy of the offense. In either case, access privileges may be revoked immediately and long-term outcomes may include temporary or permanent loss of access privileges, depending on the nature of the activities.

Acknowledgements: *The Computer Use Committee wishes to thank the University of Windsor, University of Guelph, University of Waterloo, University of Toronto, whose policy statements have contributed to this document.*