

 St. Lawrence College PROCEDURE	# of Pages 5	Procedure #: P-42
	Approved by: Executive Committee	
	Originator: Education & Information Technologies	
Title: Acceptable Use for Computing	Effective Date: February 2005	Replaces: 14 January 2002

PROCEDURE

1.0 Scope

This Procedure applies to all computing systems, facilities and resources (including any personal computer, computing or communications facility) owned or leased by, or licensed to, St. Lawrence College.

These computing systems, facilities and resources are the sole property of St. Lawrence College. The College reserves the right to determine what constitutes acceptable usage of its computing systems, facilities and resources, and to monitor usage by any individual to ensure compliance with the College's property rights, this Policy, and other legal requirements. No person covered by this policy shall have or acquire any property or privacy interest in the College's computing systems, facilities and resources, or in any information generated, stored or received on or accessed or sent using the College's computing systems, facilities and resources.

The computing systems, facilities and resources of St. Lawrence College serve to support and enhance the quality-learning environment. The use of information systems and/or computing facilities at St. Lawrence College is restricted to those functions supporting or enhancing the academic mission of the College. As a critical component of our information systems, both academic and administrative, persons using, accessing or in any way interacting with these resources are bound by the policy of Acceptable Use for Computing at St. Lawrence College. This includes any person accessing or interacting by way of any communications/computing device with the College's communications networks and or systems.

The College strictly prohibits the use of its computing resources/facilities for purposes which -

- Do not serve the academic or business endeavors of the College;
- Are harassing or discriminatory in any way;
- Are contrary to the Criminal Code or the offence provisions of any provincial statute;
- Are otherwise prohibited by law.

2.0 Definitions:

- Users - Refers to any person e.g., students, faculty, staff utilizing any system, facility or resource as defined above.
- User Account - Refers to any account number, access code, user identification or password explicitly granted for access to a computer system.

3.0 Guidelines for Acceptable Use Computing

3.1 User Responsibilities

- 1) Users are responsible for any and all use of their User Accounts. As such -
 - a) Users must maintain secure passwords for any and all accounts assigned to them.
 - b) Users must ensure and safeguard against others obtaining unauthorized access to their accounts.
 - c) Users must not share passwords or any other access control information for their accounts.
- 2) Users are responsible for ensuring the confidentiality of any restricted data or information they have been granted access to. As such -
 - a) Users must ensure that confidential information is not observed by others while users are working at a computer.
 - b) Users must not leave their computers unattended while logged on to their accounts.
 - c) Users must exercise discretion when printing confidential information which may be viewed or observed by unauthorized persons.
 - d) Users may not copy, send, duplicate or transmit by any means, confidential College data for any purpose other than performance of College related business.
- 3) Users must comply with all copyright and license conditions associated with College computing systems. As such -
 - a) Users must not move, copy or transfer programs, files or other forms of software from one computing system to another without proper authorization to do so.
 - b) Users must not distribute, sell or make available software to any person where prohibited by copyright or license.
 - c) Users must not access and use software belonging to or owned by St. Lawrence College without proper authorization and license rights.

3.2 User Restrictions

Users must use computing facilities only for the purposes for which they were authorized. As such -

- 1) Users* must not use College computing resources for personal/private business use or for any form of direct personal financial gain or the support advancement of a political or personal cause.
**Exclusion: XL Program students using his/her laptop*
- 2) Users must not use College computing resources for personal support or the furthering of political causes.
- 3) Users must not use College computing resources for the creation, transmission, storage, access or viewing of materials which in any way contribute, support or promote actions which are prohibited on the basis of harassment and/or discrimination including but not limited to the categories of:
 - a) Harassment,
 - b) Sexual Harassment,
 - c) Racial/Ethnic/Cultural Harassment,
 - d) Discrimination,
 - e) Poisoned Environment,
 - f) Hate Literature,
 - g) Systemic Harassment/Discrimination,
 - h) Reprisal.
- 4) Users must not use College computing resources for the creation, transmission, storage, access, or viewing of materials prohibited by federal and/or provincial law. These restrictions include, but are not restricted to the following:
 - a) Any form of material supporting or contributing to the harassment or discrimination as categorized in section 3.2 restriction 3).
 - b) Any form of pornographic, obscene or sexually explicit material.
 - c) Any form of illegal trade, negotiation or conspiracy to conduct illegal acts.
- 5) Users must not use College computing resources for the creation, transmission, storage, access or viewing of materials which are deemed by the College to serve no useful academic purpose.
- 6) Users must not attempt to interfere with the normal operation of College computing systems, facilities or resources. As such users must not -
 - a) Attempt to encroach on others' use of computing facilities.
 - b) Attempt to subvert the restrictions associated with their computer accounts.
 - c) Attempt to gain access to systems both within and outside of St. Lawrence College for which they have no authorization.
- 7) Users must not utilize any College computing facilities for the purpose of creation, development, storage, replication or transmittal of any program, code, subroutine or other means intended to disrupt, interfere, destroy or corrupt the normal operation of systems or data. (e.g., viruses, worms, hack-utilities, net snooping utilities).

3.3 User Rules for Computer Labs

In addition to the responsibilities and restrictions as described in Sections 3.1 and 3.2, the following user rules apply to all Academic or Public Access Computing Labs within St. Lawrence College.

- 1) Academic computing labs (teaching or general access) serve to support the teaching and learning endeavors of the College community. Users of these facilities are expected to behave in an appropriate manner so as not to disrupt in any way users of these facilities.
- 2) In accordance with section 2. Guidelines for Acceptable Use Computing, users of these facilities shall in no way participate in actions which are prohibited on the grounds of harassment, discrimination or by way of illegal act. Examples include the access, transmittal, storage or viewing of materials reasonably determined to be -

sexually explicit, pornographic, obscene, harassing or discriminatory (on the basis of race, ethnicity, culture, gender or sexual orientation), supporting or contributing to hatred of any group or in any way threatening, as perceived by any individual or group.
- 3) In order to ensure the proper functioning of these labs, users must not in any way tamper, change, or disrupt the normal function of the hardware and software contained within these facilities. Examples include such things as changing operating system configurations, desktop attributes or software functions.
- 4) Lab users shall not download, store or install any software or other electronic file which does not support an approved academic purpose, which is for personal use or for which they do not have the explicit consent to do so by an authorized College official.
- 5) Lab users must not knowingly access, store or transmit any program, code, subroutine or other electronic file which is known to contain destructive or interfering capabilities such as viruses.
- 6) Lab users must not use the printing services contained within these labs for any nonacademic, personal use e.g., flyers, internet documents, manuals etc.
- 7) Multi-copy printing is strictly prohibited. Photocopy services are located throughout the College campuses for such use.
- 8) Lab users must in no way misrepresent their identity through impersonation, alias or anonymity so as to conduct or transmit any untoward communication, data or other file.
- 9) Plagiarism, theft, cheating on tests, assignments or reports, misrepresentation of identity, or the falsification of data in any way constitutes "Academic Dishonesty". Academic Dishonesty, as described in the College Academic Policies is a serious offense and extends to the users of computing lab facilities.

- 10) Lab users must be prepared to present, upon request, College identification in the form of a current Student or Staff ID card.

4.0 Procedure for Policy Violation

The following guidelines outline the procedures and disciplinary measures which may be invoked in instances of policy violation. Progressive disciplinary measures are instituted in instances of **minor** violations. More serious offenses including but not limited to issues of harassment, discrimination, threats to personal safety, substantial risk to a College member (staff, students or visitors) or major damage to College systems will result in immediate disciplinary measures aimed at safeguarding or protecting individuals or College resources.

The process for addressing alleged violations of the Acceptable Use Policy for Computing is as follows:

- a) A first violation (**minor**) will result in a warning to cease the alleged violation. Warnings may be issued by any College employee witnessing or suspecting a violation of this policy by any student or visitor of the College. Warnings may be issued by any College Manager/Official witnessing or suspecting a violation of this policy by any staff member.
- b) A meeting may be set up to review the alleged violation, allow the individual an opportunity to respond, and to discuss the warning. In the case of the students, such meetings shall be attended by the staff member witnessing or suspecting the violation, the coordinator of the program in which the student is enrolled or the responsible Dean.
- c) A second violation will result in a written warning from the appropriate Manager, Dean, or Vice President of Education and Information Technologies. At that point the alleged violation is considered to have become a disciplinary matter and will be referred to the appropriate disciplinary body or process.
- d) In issues of student violation, the Dean of the appropriate School, in conjunction with the program coordinator shall determine the course of disciplinary action. The College's Zero Tolerance Policy on Harassment governs matters of harassment or discrimination.
- e) Third and subsequent violations will result in restriction or complete suspension of access to computing facilities. Such sanctions will remain in effect until the investigation of the alleged violation is complete. Opportunities for review and discussion of the alleged violation will be subject to the "Student Appeals Process" or in the case of staff, the provisions of the College's employee groups' Collective Agreements.
- f) Major violations will be responded to immediately. The Vice President of Education and Information Technologies retains the right to enact certain preventative measures, which could include a restriction in or complete suspension of access to computing facilities and services. In extreme cases of alleged violations, the Vice President may be forced to impose such sanctions as an immediate preventative measure until such time that an investigation has been completed.