

ACCEPTABLE USE POLICY – UNIVERSITY COMPUTING RESOURCES

POLICY No.:	002
SCOPE:	All Faculty, Staff, Administrators and Students
APPROVAL:	Board of Governors
DATE OF ORIGINAL POLICY:	October 20, 2005
LAST UPDATED:	N/A
SCHEDULED REVISION DATE:	October 2011
CONTACT:	Director, Computer Services

1 Preamble

In recognition of the contribution that computers and computing resources can make to furthering the educational and other objectives of NSCAD University (“NSCAD”), this policy is intended to promote the responsible and ethical use of NSCAD computing resources.

2 Purpose

In order to protect the best interests of the NSCAD community as a whole, these Computing Resources (including but not limited to mainframes, minicomputers, personal computers (such as Mac and PC/Windows), personal digital assistants (such as Palm or PocketPC devices), printers, peripheral devices, software, network hardware such as hubs, switches and wireless access points and access to computer networks such as the Internet) shall be used in accordance with this policy and in accordance with the terms of applicable collective agreements and codes of student conduct.

3 Scope

This policy applies to all Computing Resources owned, leased, operated, or contracted by NSCAD and used for whatever purpose (“NSCAD Computing Resources”).

Subject to this policy, system administrators of NSCAD computing facilities (including but not limited to the Director of Computing Services) may have rules

regarding the use of these facilities. Such administrators are responsible for publicizing the rules concerning the authorized and appropriate use of the computing facilities for which they are responsible.

4 Privacy

Files and personal communications, including those stored on NSCAD Computing Resources, are private.

However, with due regard for any right to privacy of users and the confidentiality of their data, system administrators of NSCAD computing facilities authorized by any Vice-President or the President may, from time to time, monitor and record computing activity in order to maintain the integrity of NSCAD Computing Resources or to comply with any legal requirement such as but not limited to court order, arbitrator's order, or criminal proceedings.

Individuals must respect the rights of other authorized users.

5 Usage Guidelines

The following activities are prohibited:

- a. Using or attempting to use another user's computer account and/or password without permission. A user is normally identified by his or her username and is responsible for all activities performed on NSCAD Computing Resources under their username. A user who reveals or allows others to use their account may be restricted in the use of NSCAD Computing Resources if others abuse NSCAD Computing Resources in their name.
- b. Interfering with the security or confidentiality of other users' files or maliciously destroying any other users' data.
- c. Impeding others or interfering with their legitimate use of NSCAD Computing Resources including, but not limited to, sending illegal, threatening, or repeated unnecessary mail messages (such as chain letters) or knowingly downloading illegal material.

- d. Using NSCAD Computing Resources to violate the terms of any software license agreement whether or not NSCAD is not a party to such agreement.
- e. Using NSCAD Computing Resources to illegally copy data that is the property of NSCAD or others or putting unauthorized or illegal software, data files, or other such computer-related material on NSCAD Computing Resources. Questions with respect to authorization should be directed to the Director of Computing Services.
- f. Attempting to interfere with any restrictions on NSCAD Computing Resources, including but not limited to unauthorized access to files or other Computing Resources.
- g. Using NSCAD Computing Resources for illegal purposes not specifically mentioned above.

6 Violations

Reasonable suspicion of a violation of the principles or practices laid out in this policy should be reported to the Director of Computing Services. Such reasonable suspicion will be investigated and may result in subsequent action. Such subsequent action will be taken through normal NSCAD channels.

7 Questions

Any questions regarding this policy should be directed to the Director of Computing Services.