

ACCEPTABLE USE POLICY OF NSAC COMPUTING RESOURCES

Fall 2006

In support of its mission to provide excellent instruction, modern research, and meaningful service, the Nova Scotia Agricultural College offers computing resources to its students, faculty, and staff. These resources contribute to the work of all members of the NSAC community and, therefore, must be used with great care.

This brochure is intended to help set the tone for computing and for the use of computing resources at the Nova Scotia Agricultural College; respect for the rights of all users and fair use by all so as to guarantee equal access to all users. The goal of the NSAC in providing computing resources is to give users powerful tools to further their academic endeavors. The privacy of all users and of all of their files is a fundamental right that should be respected by all. You should never use the computing resources in any way that violates the privacy of others. Clearly defined procedures established to protect your rights will always be followed as the NSAC maintains the computing system.

Careful and ethical use of computing resources is the responsibility of every user. As a user of these resources, you agree to be subject to the guidelines of the "Acceptable Use Policy of the Nova Scotia Agricultural College Computing Resources". These guidelines apply to all computing resources provided by the NSAC; some are related to microcomputers and local area networks, and some to all systems. This brochure includes and expands upon those guidelines, and contains a glossary of the technical terms used in the policy.

In the text that follows, the Policy itself is set in straight, bold type; comments, explanations, and expansions are set in italics.

ACCEPTABLE USE POLICY OF NOVA SCOTIA AGRICULTURAL COLLEGE COMPUTING RESOURCES

TWO BASIC RIGHTS

Access to computing resources is granted to an individual by the NSAC solely for the grantee's own use. Every user of the NSAC computing resources has two basic rights regarding computing:

1. Privacy
2. A fair share of resources

It is unethical and a violation of this policy for any person to violate these rights.

All users, in turn, are expected to exercise common sense and decency (due regard for the rights of others) with respect to the public computing resources, thereby reflecting the spirit of community and intellectual inquiry at the NSAC. Access is a right that may be limited or revoked if an individual misuses the right or violates applicable NSAC policies or provincial or federal laws.

PRINCIPLES GOVERNING USE OF COMPUTING RESOURCE

A. User access is granted to an individual and may not be transferred or shared with another without explicit written authorization by Information Technology Services, a designee, or the appropriate system administrator.

This principle is intended to protect the integrity, security and privacy of your account. Sharing access with another individual undermines the security of your account, leaving it vulnerable to abuse by others. By not sharing your account, you protect against unauthorized activities on your account, for which you would be responsible. You may be charged with a

violation if someone uses your account with your permission and violates policy. Just as important, sharing or transferring access jeopardizes the security of the entire computing system because it weakens one of the lines in the system "chain."

For more information on obtaining your own account contact the appropriate NSAC ITS Helpdesk:

NSAC ITS Student Helpdesk: 893-6308

Email: Helpdesk@nsac.ca

NSAC ITS Staff Helpdesk 893-6154

Email: Helpdesk@nsac.ca

B. User access to computing resources is contingent upon prudent and responsible use.

Imprudent use of computing resources can leave consequences affecting many other users, not just yourself. For example, not using virus protect software on networked microcomputers could allow the introduction of a virus that could destroy work of many other users.

Prudent and responsible use begins with common sense and includes respect for the rights and privacy of other users. For example, as a prudent and responsible user, you should:

1. *Not share your account with any other user.*
2. *Protect your password by choosing it wisely, keeping it secure, and changing it regularly.*
3. *Back up files on a regular basis to ensure the safety of important data in the event of a system failure.*
4. *Log off your account when leaving a work station.*
5. *Always use virus protection software.*

C. The user may not use computing resources for any illegal or unauthorized act; in particular, the user may not use computing resources to violate any provincial or federal laws or any of the regulations specified in the NSAC Calendar, the NSAC Student Handbook, Community Standards and Residence Handbook and the User Policy for NSAC Computing Services. The User Policy appears as Appendix 1 of this document. You will find copies of all of these documents in the Student Services office, the Registrar's office, and the NSAC ITS Student Helpdesk.

PRINCIPLES GOVERNING USE OF COMPUTING RESOURCES

D. The user may not use computing resources for any commercial purpose without prior written authorization from the Vice-President, Administration , a designee, or the appropriate system administrator.

Work under approved NSAC contracts and grants is covered under the usual internal approval processes, which serve as the requisite "prior written authorization." If you need to open a commercial account or would like more information, contact the appropriate NSAC ITS Helpdesk .

E. Computing resources must be shared among users in an equitable manner. The user may not participate in any behaviour that unreasonably interferes with the fair use of computing resources by another. Computing resources are finite and must be shared. During periods of peak demand, facility staff may enforce guidelines to require sharing resources for the benefit of everyone.

Examples of unreasonable interference include, but are not limited to:

1. *Playing games for recreation when another user needs the resource for more scholarly activities.*

2. *Exceeding established disk space, time, or other allocations.*
3. *Intentionally running programs that attempt to execute endless loops.*
4. *Printing large jobs during periods of heavy computer use.*
5. *Downloading large files.*

SOME EXAMPLES OF VIOLATIONS

*This section of the Policy consists of a list of several activities that you cannot or should not do. While these are not all of the possible violations, there are still many more things you can do than things you **can't** do. This list is intended to inform you and to reinforce the principles of fair and responsible computer use that we seek to engender at the Nova Scotia Agricultural College.*

Violations of these principles or any attempt to violate these principles constitutes misuse. Violations include, but are not limited to:

a. Sharing passwords or acquiring another's password without prior written authorization from Vice-President, Administration or the appropriate system administrator.

The consequences of sharing your password can be significant for the system and for you as well. This action leaves you vulnerable to such things as impersonation by another user.

However, even if you are not concerned about the safety of your own account and data, you have a responsibility to other users to help maintain the security of the system. Your responsibility is like that of a tenant in an apartment building. Though the tenant may not be concerned about his or her own apartment, feeling that it contains little or nothing of value, he or she still has a responsibility to the other tenants to keep the main entrance secure.

On occasion, you may want to share files or data or e-mail with other users. For information on how to do that safely, contact the appropriate NSAC ITS Helpdesk.

b. Unauthorized accessing, using copying, modifying or deleting of files, data, user id's, access rights, usage records, or disk space allocations.

You are authorized to access, use, copy, modify, or delete files, data or access rights on your own account as specified in the Policy. You are not authorized to perform any of these functions on another user's account or a NSAC System unless specifically given permission by the account holder, your job description, Information Technology Services or a designee.

A person who finds a door to another's home unlocked doesn't have the right to enter the home simply because it is unsecured. Similarly, the fact that someone's account and its data are unprotected doesn't mean that you have the right to access it.

c. Accessing resources for purposes other than those for which the access was originally issued, including inappropriate use of authority or special privileges.

User privacy is not to be violated; all users are to be protected from unauthorized activity by a system administrator or other users.

d. Copying or capturing licensed software for use on a system or by an individual for which the software is not authorized or licensed.

Canadian Copyright Law

NSAC supports and adheres to Canadian Copyright Law and the Educom Code. The Educom Code is as follows:

The Educom Code - Software and Intellectual Rights.

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy and right to determine the form, manner, and terms of publications and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

The Nova Scotia Agricultural College subscribes to the principles expressed in the EDUCOM Guide to the Ethical and Legal Use of Software. "Unauthorized copying and use of software deprives publishers and developers of a fair return for their work, increases prices, reduces the level of future support and enhancements and can inhibit the development of new software products."

---"Using software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community"

EDUCOM

For a printed copy of the guidelines, write or call: EDUCOM, 1112 16th St., NW. Suite 600, Washington, DC 20036, (202) 872-4200. If you are unsure about whether you possess legal software copies, contact the appropriate NSAC ITS Helpdesk for more information.

The Nova Scotia Agricultural College doesn't condone or authorize the illegal copying or possession of software. NSAC students and employees are prohibited from copying software illegally and possessing

illegal copies of software, whether for course, job related, or private use. Any violations of this policy or of Copyright law are the personal responsibility of the user. The NSAC will not assume any liability for such acts. Furthermore, Information Technology Services will refuse to provide support for a user who cannot demonstrate that the software involved was obtained legally.

e. Use of computing resources for remote activities that are unauthorized at the remote site.

For example, if you are accessing another university's system using an NSAC computing resource, you must obey that school's own computing rules. Your actions reflect upon the entire NSAC community.

f. Causing computer failure through an intentional attempt to "crash the system," or through the intentional introduction of a program that is intended to subvert a system, such as a worm, virus, Trojan horse, or one that creates a trap door.

You have a responsibility to other users to help maintain the security of the system. The intentional introduction of a subversive program is considered a grave offense. Taking reasonable precautions is part of your responsibility. If you think you may have accidentally introduced one of these programs, contact Information Technology Services. For information on virus protection software, contact the appropriate NSAC ITS Helpdesk.

g. Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction.

Header information of electronic mail, files, and printouts is an essential part of the identification and documentation of your

work. Forging electronic mail or masking identification information - for amusement, personal gain, or other reasons - is not allowed.

h. Interception of transmitted information without prior written authorization from Information Technology Services or the appropriate system administrator.

This violation is a serious invasion of another user's privacy and is analogous to tapping that person's telephone line. The NSAC respects the right to privacy of all users and endeavors to do all in its power to maintain that right. You should be aware that sometimes, in the course of system maintenance, transmissions are tracked, but the contents are not read. You should also be aware that unauthorized users of the system are not afforded this same protection from invasion of their privacy. This means that the NSAC can and will read transmissions by unauthorized users, to maintain the integrity and security of the computer resources for all authorized users.

i. Failure to protect one's account from unauthorized use (e.g., leaving one's work station publicly logged on but unattended).

When you do not protect your account from unauthorized use, you weaken the security of not only your account, but the entire system. Keeping your password secure and attending to your account when logged on are key means of protection.

j. Violation of priorities for use of computing resources as established by an individual facility within the NSAC system.

Some NSAC computing facilities may have no usage rules beyond those given in this brochure. However, many have established priorities for use of computing resources to

ensure that scholarly activities are granted more weight than, for example, recreational gameplay and other non-academic pursuits. These priorities must be respected.

RESPONSE TO VIOLATIONS

Violation of this policy will result in action by staff supervisors, the NSAC Judicial System and or law enforcement agencies.

Violations of statutes dealing with unlawful access or use of a computer may be referred to the police for investigation and/or prosecution.

NSAC SANCTIONS

NSAC sanctions are imposed by the appropriate NSAC authority and may include, but are not limited to, limitation or revocation of access rights and/or reimbursement to the NSAC for the computing and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident. The usual rights and privileges of appeal apply.

INVESTIGATION AND REVIEW OF CHARGES

When a staff member of Information Technology Services has reason to believe that a violation may have occurred, he/she may initiate an investigation through the judicial process and/or suspend computing privileges for the individual(s) involved, pending further investigation.

If significant NSAC sanctions are imposed, such action, together with an explanation of the causal events, shall be

reported by the Assistant Dean Judicial to the Dean of Students' office, in the case of students; by the Regional Infrastructure Coordinator of Information Technology Services to the appropriate Vice President's office, for all others.

Investigating officials will examine charges of violations with due respect for both individual privacy and the security of other users.

GLOSSARY

Access right: permission to use a NSAC computing resource according to appropriate limitations, controls and guidelines.

Commercial purpose: a goal or end involving the buying and/or selling of goods or services for the purpose of making a profit.

Computing resource: any computing/network equipment, facility, or service made available to users by the NSAC.

Data: a representation of facts, concepts or instructions suitable for communication, interpretation or processing by human or automatic means.

Disk space allocations: the amount of disk storage space assigned to a particular user by Information Technology Services or the appropriate system administrator.

Fair use: use of computing resources in accordance with this policy and with the rules of an individual NSAC facility; use of computing resources so as not to unreasonably interfere with the use of the same resources by others.

File: a collection of data treated as a unit.

Inappropriate use of authority or special privilege: use of one's access right(s) or position of authority in a manner that violates the rules for use of those privileges as specified by Information Technology Services, a designee or the appropriate system administrator.

Password: a string of characters that a user must supply to meet security requirements before gaining access to a particular computing resource.

Prudent and responsible use: use of computing resources in a manner that promotes the efficient use and security of one's own access right(s), the access rights of other users, and NSAC computing resources.

Remote activity: any computing action or behaviour that accesses remote site facilities via a NSAC computing resource.

Remote site: any computing/network equipment, facility, or service not part of, but connected with, NSAC computing resources via a communications network.

System administrator: any individual authorized by Information Technology Services or the Resources CSU IT Director to administer a particular computing hardware system and/or its system software.

Transmission: the transfer of a signal, message or other form of intelligence from one location to another.

Unauthorized act: with the exception of computing actions or behaviours permitted in this policy, any such act performed without the explicit permission of the Vice-President, Administration, a designee or the appropriate system administrator.

Usage record: information or data indicating the level of usage of computing resources by a particular user.

User: any individual - whether student, faculty, staff or individual external to NSAC - who uses NSAC computing resources.

User ID: a character string that uniquely identifies a particular user to a NSAC computing resource.

Note: Document to be revised not less than annually (persons/committees to be specified)