Nipissing University

Policy Category	
Policy Number	
Policy Name	**Acceptable Use Policy**
Responsible Department	University Technology Services
Original Approval Date	
Approval Authority	
Last Updated	
Next Review Date	

VALUE STATEMENT

The purpose of this Acceptable Use Policy is to provide guidelines for the appropriate use of Nipissing University's computing resources. Computing resources at Nipissing University, and the on-campus electronic communication systems by which they are interconnected and accessed, exist to support the research, instructional, and administrative needs of the University community. This community, like all communities, has rules; rules intended to ensure a safe, reliable, and consistent computing environment for all members of the University community. These rules are not merely arbitrary violations of users' freedoms. All who use the University's computing resources must act responsibly, in accordance with the highest standards of ethical and legal behaviour. Thus, legitimate use of computing resources does not extend to whatever is technically possible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

DEFINITIONS

Computing Resources include, but are not limited to, wiring or infrastructure used for communications; electronics, digital switches and communication equipment used for processing or communications; programs, programming languages, instructions, or routines which are used to perform work on a computer; digital information such as records, images, sounds, video or textual material stored on or accessible through a computer; computers used for automation or the administration of information services; information such as I.D.s, authorization codes, account numbers, usage and billing records, or textual material stored on or accessible through the network or other communication lines.

Users include the current faculty, administration, support staff, currently registered students, and others as authorized by the Vice-President, Finance & Administration (herein referred to as F & A).

BASIC PRINCIPLES

The University's network resources are provided to support academic and the University's business-related activities. It is not to be regarded as an Internet service provider and therefore does not provide unlimited or unrestricted bandwidth or access. Limitations and/or restrictions imposed upon the use of network resources are subject to change and are designed to protect the security and integrity of these resources.

Users may not share passwords, including any that may belong to others that the user may become aware of.
A user is responsible for all activity originating from his or her account and/or computer equipment, regardless of who actually may be using the account and/or equipment.

Users may not attempt to circumvent any security or resource management measures.

Attempting to discover or disclose confidential information stored on University computing facilities is not permitted.
Users may not interfere with the ability of others to use the network or other commonly shared technology.

Users may not attach more than one personal computer or laptop operating in workstation mode to a single network jack in a residence room (including studies), common areas, classrooms, or offices. It is not permissible to attach to these network jacks any other devices such as, but not limited to, fileservers, webservers, printservers, DHCP servers, hubs, routers, switches, gateways, firewalls, wireless access points, or gaming consoles (GameCube, Xbox, etc.) without the express permission of University Technology Services (UTS).

Users may not make commercial use of university network resources, such as using University email address in commercial correspondence, operating a commercial server over the University network, and/or including click-thru links or banner ads on a website hosted on the University network without the express permission of the VP.

Breaking University-published policies constitutes a breach of academic integrity and/or employment conditions. Users' access to computing services and resources may be revoked if there is a violation of these rules or their intent.

POLICY STATEMENTS

Accessibility

Only those designated as approved users will have access to the University's computer resources. Users will employ only those computer accounts for which they are authorized, and shall take all necessary precautions to prevent others from obtaining access to their computer accounts. The holder of a computer ID and password is responsible for protecting campus computing resources from unauthorized access by keeping the password confidential and changing it regularly.

All resources are intended for shared use within the University community and are to be used in a reasonable and responsible manner.

Confidentiality of Information

Each user is accountable for ensuring the confidentiality and integrity of information accessed, maintained or disseminated, consistent with the University's policies and procedures as well as federal and/or provincial laws.

Purpose of Use

The University's computer equipment, infrastructure and resources are only for University-related activities. Any and all personal use of University resources is prohibited. This includes but is not limited to, offering information or services for sale or personal gain, or to distribute advertising material, using the University network resources to provide computing services outside the University's network or to provide any external computing service to the campus community, without authorization from the University.

Pornography/Hatred/Racism

University resources are not to be used to create, transmit, store or copy information that is obscene, threatening or harassing.

Physical Security

No user or users shall, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or stored information. Any uses that unduly interfere with the work of others or with the work of host systems are prohibited. This includes, but is not limited to: unauthorized use of a computer ID or password; seeking information about or attempting to modify the Universities computer security system; and knowingly propagating computer viruses, bots, trojans, malware or electronic chain letters.

Copyright

All software, in any medium, is protected under the Criminal Code of Canada. Any copying of software, except as expressly stated in the licensing contract of the software, is prohibited. Users must respect copyrights, intellectual-property rights, ownership of files and passwords. Unauthorized copying of files or passwords belonging to others or to the University may constitute plagiarism and/or theft. Accessing or modifying files without authorization (including altering information, introducing viruses or trojans, or damaging files) is unethical, may be illegal, and may lead to sanctions. The University will not be held liable for any breach of copyright and furthermore, will assist any software supplier with just cause, to prosecute any individual violating the copyright laws.

Electronic Mail

It is the user and not the University that is responsible for his or her electronic mail contents and his or her decision to read a mail message. It should be assumed that the contents of any electronic message are not secure and the user should take appropriate measures in regard to the contents and handling of any electronic messaging.

Penalties

Any misuse of the computing resources may lead to disciplinary action within the University's established policies and procedures; any misuse may also lead to civil and/or criminal action.

When an abuse of the acceptable use policy is suspected, the F & A has the right to conduct a preliminary examination. This examination may involve files, programs, or tapes, and will not be confined to the physical parameters of files.

Upon further investigation, the F & A may temporarily withdraw computing privileges. Any user under suspension shall receive written notice of such, giving precise grounds for suspension along with a plan of investigation.

The F & A has the right to impose penalties if the due process has confirmed the abuse. The normal penalty will be withdrawal of access to the University's computing facilities and resources. Investigation and penalties may extend beyond that of the University to include local city police, the Ontario Provincial Police and/or the R.C.M.P. if warranted by the alleged abuse of the University's Acceptable Use Policies.