

**Approved by IT Advisory Committee:**  
**Approved by Executive Committee:**  
**Approved by President's Council:**

**June 9, 2000**

**June 16, 2000**

# **NAIT *Guidelines***

**OA.6.21**

## **For Internet Use and Security Standards**

Replaces: New

Implementation Date: June 16, 2000

### **Table of Contents**

<b>Section</b>	<b>Description</b>	<b>Page</b>
1.0	Definitions	1
2.0	General Usage Guidelines	2
3.0	Acceptable Connectivity	3
4.0	Employee Policy and Standards Agreement	5

**Purpose:** This document is intended to identify the circumstances under which a NAIT employee or student may access or use the Internet through NAIT equipment and facilities. The purpose is to clearly define and communicate NAIT's expectations with respect to acceptable Internet usage and conduct.

**Scope:** This standard of practice applies to all NAIT employees or students who may access or use the Internet through Institute or other facilities, including employee or student owned systems when they identify themselves as a NAIT employee or student.

## **Standards of Practice Overview**

Access to the Internet by NAIT employees and students and duly authorized representatives is permitted and encouraged in cases where such use is both suitable for business or learning purposes and supports the goals and objectives of NAIT. It should be understood that the infrastructure required to provide this access represents a sizeable commitment of resources by NAIT. Unnecessary Internet usage causes network and server congestion and additional cost and is to be avoided.

Additionally, NAIT may be exposed to unfavourable publicity or legal liabilities due to the misuse of this resource. The purpose of this document is to help NAIT employees and students understand what is expected regarding the use of this resource and to protect NAIT, employees and students. It should be made clear that this standard of practice is in addition to all current NAIT policies and that all existing NAIT policies apply equally to the use of the Internet.

## **1.0 Definitions**

### **1.1 General Internet Related Definitions**

Browser – A computer program which allows one to access web and FTP servers. Netscape Navigator, Netscape Communicator, and Microsoft Internet Explorer are examples of these programs. Just having this program does not necessarily allow one to actually access the Internet.

Hacking/Cracking - Attempting to access another system on which you have no authorized personal access granted, and is treated as malicious intent. Also includes masquerading as an authorized user or forging messages so as to appear to be from another person.

E-Mail – Electronic mail. The company system used for electronic communications is Lotus Notes. In addition to providing internal communication functionality, it is connected to the Internet and can send and receive messages to other Internet connected e-mail systems using the SMTP (Simple Message Transfer Protocol) standard. However, in the context of this standard, this includes any other e-mail system that communicates over the company owned network or any service that the company pays for. This includes, for example, any POP3 or IMAP4 mailer such as Eudora, Microsoft Internet Mail, Microsoft Outlook, Netscape Messenger, or other proprietary mail systems such as CompuServe or AOL.

Internet – The publicly accessible interconnected worldwide network of computers and servers not owned by NAIT. Example services commonly available on the Internet are: World Wide Web, WWW or HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), Telnet, Usenet.

Intranet – The network of computers and servers owned by NAIT, including any web servers that are accessible only within our own network.

Mailing Lists – similar to Usenet groups, but is accessible using only the e-mail system.

Spam – Unwanted e-mail messages, typically trying to promote X rated web sites or sell something or solicit involvement in pyramid ‘get rich quick’ schemes. These messages are commonly sent to you after you have sent a message to a public Usenet group or mailing list.

Usenet – Also called Usenet Groups, Network news groups or NNTP (Network News Transport Protocol). A type of ‘bulletin board’ system on the Internet where all individuals participating can see all the messages posted by everyone else. Accessing these messages requires the use of special software.

## **2.0 General Usage Guidelines**

### **2.1 Understand the Level Of Security**

The integrity of confidential or proprietary information sent onto the public Internet can not be assumed. Prior approval from management will be required before NAIT confidential or proprietary information can be transmitted over or posted to the Internet.

### **2.2 Communications to the Internet May be monitored**

- a) Users are specifically advised that they should have no expectation of privacy for any Internet based communications (such as email), whether business or personal. Once information is onto the Internet it may be intercepted and read by any third party.
- b) Users are further advised that information passing through the corporate link to the public Internet (external communications) may be intercepted and/or monitored by NAIT’s Network Infrastructure Services. NAIT has in place systems and software that can monitor and record (for each and every user) each WWW visit, email, telnet, file transfer out of our internal networks and reserves the right to use this facility to ensure compliance with the Guidelines for Internet Use and Security Standards. However, the Institute will not conduct general or secret monitoring of staff regarding the content of electronic files or mail except for law enforcement purposes or, with the approval of the Manager of Security Services, where allegations of inappropriate use have arisen

### **2.3 Maintain Professionalism**

External communications must not be inflammatory, harassing, defamatory or disruptive to their companies, organisations or individuals, or otherwise reflect poorly on NAIT’s reputation or image. Personal opinions addressed to public groups, government officials, or other companies and organisations on the Internet from a NAIT employee who identifies him/herself as a NAIT employee or personal opinions transmitted using NAIT facilities must include the following disclaimer:

*“The views expressed here are mine and do not reflect the official position of my employer or the organisation through which the Internet was accessed.”*

### **2.4 Logo/Name use must be Approved**

The use on any web site of the Institute’s name, logo or wordmark must be in accordance with the NAIT Corporate Image Policy and Guidelines. Any other proposed usage, including the use of the corporate name “NAIT”, requires written approval of the Director, External Relations.

### **2.5 Standards of Web Site Development**

- a. External Relations, through the Web Communications Specialist, has the responsibility of developing the visual/contextual look and feel of the NAIT external web site at <http://www.nait.ab.ca> based on the Institute’s Corporate Identity. NAIT department and academic areas with web sites posted on the external site need to work with the Web Communications Specialist to ensure an overall consistent look and feel.

- b. The *NAIT W3 Team Report to Executive Committee, January 28, 1998* recommended that NAIT full time and apprenticeship programs be “Identified and communicated correctly in a consistent, clear and professional manner.” In order to meet this directive, the ProPage development system has been created for use by program areas to develop a dynamic and professional web site. To ensure accurate information at all times, programs should not duplicate the information contained in their ProPage elsewhere in web site development pertaining to their program. Details on developing a ProPage can be found at: <http://propage.nait.ab.ca>.

### **2.6 Personal Responsibility**

Users are individually responsible for understanding and respecting the Guidelines for Internet Use and Security Standards. Users are personally accountable for their own behaviour and responsible for any unapproved charges associated with billable services. This applies not only to NAIT systems and networks, but also to any other system accessed from the Institute network or systems.

### **2.7 Illegal Use**

Use of the Internet to transmit any material that intentionally or unintentionally, violates any applicable local, provincial, national or international law is prohibited.

### **2.8 Corrective Action**

Abuse of email and/or network privileges can result in disciplinary action ranging from a warning through suspension of network access to dismissal from NAIT, depending on the circumstances of the incident. Student disciplinary action can be taken in accordance with the Academic Regulations and Procedures. Users who violate systems or network security, or who violate these guidelines may incur criminal or civil liability, in addition to disciplinary action by the Institute. The Institute will cooperate fully with investigations of violations of systems or security at the Institute and at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.

## **3.0 Acceptable Connectivity**

All access to the NAIT Network from the Internet must be through a firewall or firewalls that have been selected and implemented by the Network Infrastructure Services group. In cases where direct dialup is absolutely required (and approved) all equipment used will be disconnected from the NAIT network. (ie. no direct modems allowed for security reasons)

### **3.1 Acceptable Uses**

There are many possible uses for the Internet. The following list is an example of what is considered acceptable use.

- Communication and exchange of information for professional development.
- For professional activities and work related associations.
- Research & Development of any work related activity, service or product.
- To remain professionally current and debate issues in a field of knowledge.
- Business travel related activities (hotels, restaurants, etc.)
- Reasonable use of the Internet for private or personal business
- Research and learning enhancement by students and staff.

### **3.2 Unacceptable & Unethical Uses**

The following are examples of inappropriate uses of the Internet and are by no means exhaustive. Users are expected to use sound judgement and if in any doubt as to the acceptability of an intended use, to discuss the matter with their manager, an IT manager, HR or instructor.

- Illegal activities of any kind
- For-Profit activities not sanctioned by NAIT
- Online gambling
- Downloading and/or viewing of pornography
- Downloading and/or storing of hacking tools
- Electronic harassment of any kind
- Seeking to gain unauthorized access to internet resources - (Hacking)
- Alteration or destruction of computer based information
- Compromising the privacy or integrity of users or the confidentiality of data
- Destructive practices or behaviour - (e.g. Spamming)
- Downloading or distributing pirated software
- Uploading or transferring NAIT source code to unauthorized person(s)/company(s)
- Copying or transmitting confidential information of NAIT, its clients or its suppliers
- Unauthorized access to internal systems and information.

## EMPLOYEE INTERNET GUIDELINES AND STANDARDS AGREEMENT

**SUBJECT: Acceptable Use of Information Technology Tools (Internet, e-mail, etc)**

Employees are encouraged to use Information Technology tools for research, education, and communications, provided it is for NAIT related business. Use for business purposes is when accessed from any computer or related equipment owned by and located on NAIT property. Professionalism is of utmost importance.

- Users should not say, do, write, view, transmit, retrieve, save, or print anything that they would not want to be viewed by others.
- NAIT employees must honor copyright laws regarding protected commercial software, ownership of information, or intellectual property.
- Individual NAIT employees who use the Internet should minimize unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource.
- NAIT employees will assume responsibility for any charges associated with any related billable services unless appropriate departmental authorization for said services has been obtained in advance.
- NAIT employees cannot use Information Technology Tools or wide area network services for any illegal purpose. This includes unauthorized access to protected resources of the Institute.
- Transmitting unprofessional communications or using NAIT resources for unsolicited advertising for personal gain is strictly prohibited.

Every employee that uses NAIT's Internet gateway or e-mail system must be authorized and registered through Information Services Division (ISD).

The Institute sets standards and guidelines. Employees will be required to follow them for consistency across the Institute.

### **Disciplinary Action**

Any violation of the internet guidelines and standards or misuse of services will result in appropriate disciplinary action up to and including termination.

I have read and understood the Guidelines document and agree to abide by the terms and conditions of this Agreement. I understand that I may be subjected to disciplinary actions if I violate the Institute guidelines.

---

Employee Signature

---

Date