

 DALHOUSIE UNIVERSITY <i>Inspiring Minds</i>	INFORMATION TECHNOLOGY SERVICES	<i>Instruction Number:</i> 5.1.1
	<i>Subject:</i> Use of IT Resources	<i>Date Issued:</i> 2009 March 19
	<i>Title:</i> Acceptable Use Policy	<i>Date Revised:</i>
	<i>Issued by:</i> Assistant Vice-President, Information Technology Services	<i>Approved by:</i> Vice-President Finance and Administration

A. PURPOSE

The purpose of this policy is to outline appropriate use of Information Technology Resources owned, leased, controlled and/or operated by the University.

B. APPLICATION

This policy applies to all individuals who have been granted a Net ID and/or Banner account by the University.

This policy does not replace other policies, procedures or guidelines concerning the use of specific IT Resources or data management but rather sets out a minimum standard of acceptable use.

C. DEFINITIONS

In this Policy,

“User Account” means a Net ID and/or Banner account issued by the University;

“Information Technology Resources”, or “IT Resources”, means computing equipment, peripherals, facilities, networks or systems owned, leased, controlled or operated by the University, including those purchased through research funds;

“User” means an individual who has been issued a User Account.

D. POLICY

1.0 Accounts

- 1.1 Authorized access to IT Resources requires a User Account. User Accounts are non-transferrable.
- 1.2 Users are responsible for any and all uses of their User Account and are expected to take reasonable steps to ensure the security of their User Account.

2.0 Acceptable Use

- 2.1 Users shall use IT Resources for authorized purposes only.
- 2.2 No User shall use IT Resources for any disruptive or unauthorized purpose, or in a manner that violates any law, University regulations, policies or procedures. Examples of unacceptable uses of IT Resources include, but are not limited to, the following:
 - 2.2.1 using another person’s User Account, or misrepresenting themselves as another User;
 - 2.2.2 disclosing passwords or other access codes assigned to themselves or others;
 - 2.2.3 interfering with the normal operation of IT Resources by, among other things, unauthorized network interception, network traffic, flooding the network with messages, sending chain letters or pyramid solicitations;
 - 2.2.4 copying, removing or distributing proprietary software and/or data without authorization;
 - 2.2.5 breaching terms and conditions of software licensing agreements;
 - 2.2.6 accessing, displaying, transmitting, or otherwise making available information that is discriminatory, obscene, abusive, derogatory, harassing or otherwise objectionable in a university setting;
 - 2.2.7 destroying, misplacing, misfiling, or rendering inoperable any stored information on a University administered computer or other information storage, processing or retrieval system;
 - 2.2.8 using IT Resources for profit or commercial gain; and
 - 2.2.9 attempting to or circumventing security facilities on any system or network.

3.0 Consequences of Unacceptable Use

- 3.1 If there is reason to suspect that a User has violated this policy, the Assistant Vice-President, Information Technology Services or the Information Security Manager may temporarily revoke or restrict User Account access privileges of any User, pending further investigation by the Information Security Manager.
- 3.2 To aid in the investigation of a suspected violation of this policy, the Information Security Manager may examine a User’s User Account information, including, but not limited to, emails, files, and any other material or data connected with the User Account, provided that s/he obtains the Assistant Vice-President Information Technology Services’ prior written approval. If the User in issue works within the Information Technology Services Department, then approval must be obtained from the President.
- 3.3 If the investigation concludes that a violation of this policy has occurred, the Assistant Vice-President Information Technology Services may restrict, suspend or revoke the User’s access to any or all of the University’s IT Resources, and may
 - 3.3.1 in the case of students, initiate disciplinary proceedings under the Code of Student Conduct; or
 - 3.3.2 in the case of employees, refer the matter for consideration of discipline in accordance with applicable collective agreements or human resource policies, as appropriate.