DALHOUSIE UNIVERSITY	*Policy Sponsor:* *Vice-President Finance and Administration*	*Approval Date:* *March 19, 2009*
Acceptable Use Policy	*Responsible Unit:* *Information Technology Services*	*Amendments:* *February 20, 2020*

A. Background & Purpose

Information and Communication Technology is a broad and continuously developing environment that, intentionally or not, can be utilized in a manner that does not further the University mission or advance its core values.

The purpose of this policy is to define the responsibilities of members of the University Community with respect to the acceptable use of University Information Technology Resources and outline the potential consequences to violation of this policy.

B. Application

The policy applies to all members of the University Community, hereinafter referred as a "User", who:

1) accesses Information under the responsibility of Dalhousie University or
2) utilizes Information Technology resources (e.g. devices, data or voice network) owned, leased, controlled and/or operated by Dalhousie University
    a. within the control and responsibility of Dalhousie University (e.g. internal networks and systems) or
    b. to connect and interact with IT resources outside of the control and responsibility of Dalhousie University (e.g. internet, personal IT resources, partner networks/systems)

C. Definitions

In this Policy:

"Information Technology Resources" refers to all networks, information systems, communication and collaborations tools, and technology support services that empower the university

"University Community" refers to all persons who are directly, or indirectly, affiliated with Dalhousie University. For example: students, faculty, alumni, operational staff (full-time and contractors), guests.

"User" refers to any member of the University Community who has any level of access to Dalhousie's Information Technology Resources.

D. <u>Policy</u>

A User is expected to comply with 5 areas of acceptable use: Legally, Respectfully, Ethically, Securely, Generally Responsible.

1.0 Legally
- 1.1 A User is responsible to use IT resources legally.
- 1.2 Legal activity requires the User to respect applicable Canadian and International Laws including, but not limited to:
  - 1.2.1 Canadian Criminal Code
  - 1.2.2 Canadian Copyright Act
  - 1.2.3 Freedom of Information and Protection of Privacy Act (FOIPOP)
  - 1.2.4 Personal Information Protection and Electronic Documents Act (PIPEDA)
  - 1.2.5 Personal Information International Disclosure Protection Act (PIIDPA)
  - 1.2.6 Personal Health Information Act (PHIA)
- 1.3 Example(s) of unacceptable activity, because it is not legal:
  - 1.3.1 Copying, removing, or distributing proprietary software and/or data without authorization;
  - 1.3.2 Breaching terms and conditions of software licensing agreements.

2.0 Respectfully
- 2.1 A User is responsible to use IT resources in a manner that is respectful of the rights of those comprising or interacting with the Dalhousie University Community.
- 2.2 Respectful behavior requires the User to adhere to the following:
  - 2.2.1 Nova Scotia Human Rights Act
  - 2.2.2 Accommodation Policy for Employees
  - 2.2.3 Personal Harassment Policy
  - 2.2.4 Sexual Harassment Policy
  - 2.2.5 Statement on Prohibited Discrimination
  - 2.2.6 Student Accommodation Policy
  - 2.2.7 Code of Student Conduct
- 2.3 Examples of unacceptable activity, because it is not respectful:
  - 2.3.1 Accessing, displaying, transmitting, or otherwise making available information that is discriminatory, obscene, abusive, derogatory, harassing or otherwise objectionable in a university setting.

3.0 Ethically
- 3.1 A User is responsible to use IT resources in a conduct that aligns with the established set of moral values of the Dalhousie University Community.
- 3.2 Ethical conduct respects, but is not limited to, the following:
  - 3.2.1 Ethical Conduct Policy
  - 3.2.2 Scholarly Misconduct Policy

3.2.3 Code of Student Conduct
3.2.4 Academic and/or Professional Standards
3.2.5 Collective Agreements (i.e. CUPE, DFA, NSGEU, PSAC)
3.2.6 Individual Terms of Employment

3.3 Example(s) of unacceptable activity, because it is not ethical:
3.3.1 Unauthorized use of IT Resources for profit or commercial gain.

4.0 Securely

4.1 A User is responsible to use IT resources in a manner that does not intentionally, or unintentionally, compromise the security of the Dalhousie University Community.

4.2 Secure activity respects, but is not limited to, the following ITS Security policies:
4.2.1 Data Administration Policy
4.2.2 Disclosure of Information Policy
4.2.3 Guest Access Policy
4.2.4 Mobile Device Policy
4.2.5 Networking Extension Policy
4.2.6 Passwords Policy

4.3 Examples of unacceptable activity, because it not secure:
4.3.1 Using another person's User Account, or misrepresenting themselves as another User;
4.3.2 Disclosing passwords or other access codes assigned to themselves or others;
4.3.3 Attempting to or circumventing security facilities on any system or network.

5.0 General Responsibility

5.1 A User is responsible to use IT resources in a manner that considers and respects the IT resource requirements of other Users.

5.2 Responsible activity respects, but is not limited to, the following:
5.2.1 Environment Health and Safety Policies

5.3 Examples of unacceptable activity, because it is not responsible:
5.3.1 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;
5.3.2 Destroying, misplacing, misfiling, or rendering inoperable any stored information on a university-administered computer or other information storage, processing or retrieval system.

Consequence of Unacceptable Use

If there is reason to suspect that a User has violated this policy, the Assistant Vice-President, Information Technology Services or the Information Security Officer may temporarily revoke, or restrict User Account access privileges of any User, pending further investigation by the Information Security Officer.

If the investigation concludes that a violation of this policy has occurred, the Assistant Vice-President, Information Technology Services or the Information Security Officer may restrict, suspend or revoke the User's access to any or all the University's IT Resources, and may:

1. In the case of students, initiate disciplinary proceedings under the Code of Student Conduct; or
2. In the case of employees, refer the matter for consideration of discipline in accordance with applicable collective agreements, human resource policies, or research contracts, as appropriate, or
3. Refer the matter to the Dalhousie Legal Counsel Office or Privacy Officer

E. Administrative Structure

Assistant Vice-President, Information Technology Service is responsible to record, and authorize the investigation of incidents of policy violation reported by the University Community or identified through system administrative activity.

To aid in the investigation of a suspected violation of this policy, the Information Security Officer may examine a User's Account information, including, but not limited to, emails, files, and any other material or data connected with the User Account, provided they obtain the Assistant Vice-President, Information Technology Services' prior written approval.

If the investigation concludes that a violation of this policy has occurred, the Academic Head, Research Services, Department Head, Human Resources, Legal Counsel, and/or Privacy Office may be engaged as appropriate in the Non-Compliance Procedure.

F. Procedures

ITS will publish additional information in the form of IT Protocols and Guidelines. This amplifying information is available on the Information Technology Services internal website at https://dalu.sharepoint.com/sites/its under IT Protocols and Guidelines.