Carleton University
Canada's Capital University

Policy Name:	Acceptable Use Policy for Information Technology (IT)
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	June 2008
Last Updated:	April 2018
Mandatory Revision Date:	April 2023
Contact:	Chief Information Officer (CIO)

Policy:

Carleton University provides IT resources to the campus community of students, faculty, staff, contractors, visitors, alumni and retirees. Provision of access to these resources requires users to act responsibly to ensure that all IT resources as well as external systems accessed from the Carleton University network, are not abused or used for inappropriate or illegal activities.

Purpose:

To ensure that reasonable steps are taken to protect the Carleton University IT resources from malicious activity and inappropriate use, and that Carleton's use of the Internet does not adversely affect other organizations or individuals.

Scope:

This Policy applies to all IT resources of the University including networks, information systems, applications and information assets.

This Policy applies to all individuals and organizations that use the Carleton University IT resources from on campus or off campus, and to all IT resources provided by Carleton University.

Procedures:

Carleton University provides access to IT resources with the expectation that users will use these resources in a responsible manner. Appropriate use of the Carleton University computing resources includes but is not limited to:

- Use of IT resources for the purpose for which they are intended;
- Adherence to the rules governing the use of IT resources as established by Carleton University;
- Respect for the property of others;

- Reporting any occurrences of misuse of IT resources to University authorities;
- Consideration of other persons using shared IT resources and facilities; e.g., student labs;
- Maintaining the confidentiality of passwords, other account information and data provided to users; and
- Adhering to software license agreements as applicable

Inappropriate use of the Carleton University computing resources includes, but is not limited to:

- Unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software or other IT resources;
- Use of Carleton University IT resources to gain unauthorized access to, or deliberately impair the functioning of any computer system or IT resource;
- Violation of software license agreements when using software on IT resources;
- Deliberate over-extension of the resources of a system or interference with the normal processing of a system; e.g., deliberate attempts to make an IT resource unavailable to its intended users;
- Unauthorized disclosure of confidential passwords and/or access devices or information for accounts, equipment and telephone voice mail;
- Development of any 3rd party website or service that requires users to submit their Carleton username/password for access, without formal consent of Carleton University;
- Unauthorized use of university facilities and resources for commercial purposes or personal gain;
- Use of IT resources to facilitate propagation of hate material or literature;
- Use of IT resources to facilitate any form of harassment;
- Theft or misuse of resources;
- Malicious or unethical use, including inappropriate, malicious or unethical use of social media;
- The creation of or distribution of malicious software including but not limited to viruses, worms, Trojans, spyware, rootkits and adware, etc., that affects the confidentiality, integrity or availability of university IT systems or data;
- Use that violates provincial, federal or international laws or statutes.

Legitimacy of Use

In the University environment, there may be legitimate reasons for conducting some activities which would typically be considered "inappropriate use" for legitimate research purposes. In the event that a user has a legitimate reason to use IT resources in a manner which violates this Policy, he/she must obtain prior written approval from the department responsible for the management of the IT resources prior to using the resources for these purposes.

Privacy

The provision and support of IT resources must be done in a manner that is fully compliant with the Freedom of Information and Protection of Privacy Act (FIPPA), an Ontario statute; and the Personal Information Protection and Electronic Documents Act, Canada (PIPEDA), a federal statute. The communication of personal information on the web must comply with the applicable provisions of FIPPA and PIPEDA. Inquiries regarding privacy and this statement are to be directed to the Privacy Office.

Users should expect and understand that there is no guarantee of privacy when using Carleton IT resources. Carleton University reserves the right to monitor the use of resources provided and/or managed by the University for the purposes of determining adherence to this Policy and applicable law. Access to IT resources may be required in support of any number of reasons including but not limited to: troubleshooting and technical support, leave of any type, security, criminal or legal investigation and freedom of information requests.

Roles and Responsibilities

All individuals and organizations that use Carleton University IT resources from on campus or off campus are responsible for ensuring their use of Carleton University IT resources is in compliance with this policy.

Compliance

Non-compliance to this Policy may result in disciplinary action and/or removal of access to IT resources.

Contacts: Chief Information Officer, ITS

Links to Related Policies: http://www.carleton.ca/secretariat/policies/

- Student Rights and Responsibilities Policy
- Human Rights Policy and Procedures