



## 9.1 Use of Information Technology

**WILFRID LAURIER UNIVERSITY**

Waterloo | Brantford | Kitchener | Toronto

---

<b>Approving Authority:</b>	Board of Governors
<b>Original Approval Date:</b>	December 6, 1990
<b>Date of Most Recent Review/Revision:</b>	November 20, 2014
<b>Office of Accountability:</b>	<a href="#">Vice-President: Academic</a>
<b>Administrative Responsibility:</b>	<a href="#">Office of Information and Communication Technologies</a>

### PURPOSE

- 1.01 This policy is presented to provide guidance and expectations to all members of the university community who provide and use Wilfrid Laurier University ("Laurier") information technology in the conduct of study, research, teaching and administration. It is based on the premise that all members of the Laurier community act in a responsible and professional way.

### DEFINITIONS

- 2.01 **Laurier information technology** includes, but is not limited to, any:
- a) computing or communication devices and associated peripherals, including desktop computers, portable computers, mobile, handheld or wearable devices, video and other multimedia devices, classroom technology, facsimile machines, scanners, copiers, printers, and telephones
  - b) computing or communications infrastructure and related equipment, including servers, switches, wired and wireless networks
  - c) programs or software, including desktop applications, mobile apps, websites, and online or cloud-computing services
  - d) services and accounts including Internet and intranet access, email, network storage, and voicemail
- that is owned, managed, hosted, or provided by Wilfrid Laurier University or a third-party provider on Laurier's behalf.
- 2.02 **Restricted access** Laurier information technology includes, but is not limited to, any Laurier information technology:
- a) that requires inputting a user-specific password in order to gain access to the technology
  - b) that provides access to any records that fall within the scope of Policy 10.1 Information Availability & Privacy Protection Policy
- 2.03 **Users** are any persons who access and use Laurier information technology, including students, faculty, staff, and alumni amongst others.

### JURISDICTION/SCOPE

- 3.01 This policy applies to all users of Laurier information technology and to all uses of said technology, whether physically located on campus or remotely.
- 3.02 This policy applies to personal information technology only when such technology is used to access or interact with Laurier information technology. Some other uses of personal information technology are governed by other policies and procedures, including, but not limited to, 9.3 Policy on the Classroom Use of Electronic Devices, the Cell Phone Program, and by the BYOD Terms and Conditions

### POLICY

- 4.01 **General rules**  
Use of Laurier information technology is circumscribed by applicable federal and provincial law, other Laurier policies, and the terms of applicable contracts and licenses. The terms and conditions in software licenses vary considerably. The onus is on users to familiarize themselves with their responsibilities and abide by limitations under each agreement.

The University has the right and the ability to access information on its systems for a wide variety of legitimate reasons, including:



## 9.1 Use of Information Technology

**WILFRID LAURIER UNIVERSITY**

Waterloo | Brantford | Kitchener | Toronto

- a) to engage in technical maintenance, repair and administration
- b) to meet legal requirements to produce information, including electronic records
- c) to ensure continuity of work
- d) to prevent or investigate misconduct and ensure compliance with the law and the University's policies

### 4.02 **Access rights**

Laurier information technology resources and tools are made available to faculty and staff in support of their teaching, research, and administrative activities and to students in support of their respective academic objectives and requirements. Access to and use of restricted access Laurier information technology by any outside party requires prior approval from the Office of the Chief Information Officer, or a designate.

Some incidental personal use of Laurier information technology by users is acceptable, but any such use should be kept to a minimum and should not interfere with University objectives or requirements. Incidental personal use of Laurier information technology is a privilege, not a right.

When outside professional activities would involve more than incidental use of Laurier information technology, approval from the user's manager or Dean (as appropriate) shall be requested in advance. Final approval shall be obtained from the Office of the Chief Information Officer, or a designate, and charges shall be at the prevailing rate (unless an agreement is made to waive all or part of the charges).

### 4.03 **Privacy**

Users are expected to use Laurier information technology in a manner that preserves the privacy of others. Users shall not:

- a) disclose confidential passwords, access codes, account numbers or other authorization assigned to them
- b) attempt to gain access to the files, file systems, or accounts of another user without clear authorization from the other user.
- c) attempt to gain access to university records without clear authorization from the data owner.
- d) attempt to intercept any network communications, such as electronic mail or instant messages.
- e) attempt unauthorized access or otherwise interfere with computing and communication installations external to Wilfrid Laurier University using Laurier information technology.

The University will meet its purpose by acting reasonably, but in light of the primary functions of Laurier information technology resources and tools, users should understand that there is no guarantee of privacy.

### 4.04 **Inappropriate use**

Users must use Laurier information technology only for the purposes for which they were authorized. Malicious, destructive, or illegal activity engaged in by users with or to Laurier information technology is unacceptable. By way of illustration only, some examples of such activities include:

- a) impersonating other individuals in communications.
- b) attempting to capture or decode passwords or encryption.
- c) theft, destruction or unauthorized alteration of data, programs, or hardware belonging to or licensed to other users or the university.
- d) willful introduction of computer viruses into Laurier information technology systems.
- e) restricting or blocking access to Laurier information technology by legitimate users.



## 9.1 Use of Information Technology

WILFRID LAURIER UNIVERSITY

Waterloo | Brantford | Kitchener | Toronto

- f) accessing, downloading, or distributing any material that would contravene any applicable regulation or legislation.

### 4.05 Harassment and discrimination

Users bear the primary responsibility for their use of Laurier information technology. Users must not use Laurier information technology to create, access, send, display, or print materials or media that either do or are likely to:

- a) create an atmosphere of discomfort or harassment for others in public shared facilities.
- b) contain obscene or harassing messages
- c) contravene relevant policies or statutes.
- d) bully or cyber-bully others whether through misuse of power, or through any means intended to offend, intimidate, insult, undermine, humiliate, denigrate or injure.

Users are directed to the provisions of the Ontario Human Rights Code and the Criminal Code of Canada for assistance in determining whether any images, sounds, videos or messages may be considered harassing or obscene. Further assistance in this regard may be obtained from policy 6.1 Prevention of Harassment and Discrimination.

### 4.06 Email and electronic communications

Users of email, social media accounts, and other electronic communications tools and services, either accessed through or provisioned as Laurier information technology, are required to use these resources in a responsible manner consistent with other business communications.

Irresponsible and inappropriate use of email includes, but is not limited to:

- a) 'rebroadcasting', i.e. forwarding email that is deemed confidential by the sender to third parties
- b) posting materials that contain virus hoaxes or spam
- c) sending email in such a way that disrupts normal email service
- d) sending materials that are fraudulent, defamatory, harassing or of a threatening nature
- e) unlawfully soliciting or exchanging copies of copyrighted material by email
- f) misrepresentation or failure to accurately identifying oneself as the sender of the email

Staff and faculty users should clearly identify themselves through an email signature that specifies their name, position, and contact information; this can also include an affiliation with another institution or agency connected with their official work, if any.

### 4.07 Consequence of violation

Users who violate these principles may be subject to disciplinary action. Any violation of this policy should be reported immediately to a user's manager or dean, as applicable, or to the Office of the Chief Information Officer, or a designate, in the absence of such a person. Users unsure of whether their intended use Laurier information technology violates these principles should consult with the Office of the Chief Information Officer, or a designate.

## RELEVANT LEGISLATION

- 5.01 [Copyright Act of Canada](#) (R.S.C., 1985, c. C-42)
- [Criminal Code of Canada](#) (R.S.C. 1985, c. C-46)
- [Canada's anti-spam legislation](#) (S.C. 2010, c. 23)
- [Human Rights Code of Ontario](#) (R.S.O. 1990, c. H.19)
- [Freedom of Information and Protection of Privacy Act of Ontario](#) (R.S.O. 1990, c. F.31)

## RELATED POLICIES, PROCEDURES, & DOCUMENTS

- 6.01 Related Procedures:
  - Bring Your Own Device ("BYOD") Terms and Conditions



## 9.1 Use of Information Technology

WILFRID LAURIER UNIVERSITY

Waterloo | Brantford | Kitchener | Toronto

---

Policy Agreement Process

[Cell Phone Program](#)

6.02 Related Policies:

[3.1 Telephone Services](#)

[3.3 Publication of Information via the World-Wide Web](#)

[3.4 Data Classification and Information Management](#)

[6.1 Prevention of Harassment and Discrimination](#)

[9.3 Policy on the Classroom Use of Electronic Devices](#)

[9.4. Information Security Policy](#)

[10.1 Information Availability and Privacy Protection](#)

[12.2 Student Code of Conduct and Discipline](#)