

## LU Electronic Services Acceptable Use

<b>Office of Administration:</b>	Office of the Chief Information Officer
<b>Approval Authority:</b>	Executive Team
<b>Approval Date:</b>	March 25, 2013
<b>Last Review:</b>	October 23, 2013
<b>Next Review:</b>	June 2015

### 1. Purpose

- 1.1 This Policy is intended to govern the use of Laurentian University's electronic services, and
- 1.1.1 To provide clear definition of what constitutes improper use of Laurentian University's electronic services.
- 1.1.2 To provide clear information of the consequences of violating this Policy.
- 1.1.3 To supersede any other acceptable use policy(ies) or statement(s).

### 2. Scope

- 2.1 This Policy applies to all staff, faculty, students, partners (such as board members and partner faculty) of Laurentian University and individuals (e.g. visitors) using a temporary Laurentian account.
- 2.2 This Policy is applicable when accessing all University electronic services including but not limited to:
- Email,
  - LUnet,
  - Learning Management System (LMS) (e.g. D2L),
  - Library via proxy access,
  - Wireless system,
  - Webadvisor and Ellucian (Datatel),
  - LU owned social media accounts,
  - Access to Internet, and,
  - LU electronic services such as FTP and others.

### 3. Definitions

3.1 The following definitions form part of this Policy:

**Confidential Information:** refers to any information that is not intended to be publicly available;

**Personal Information:** refers to recorded information about an identifiable individual including:

- information relating to race, national ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- any identifying numbers, symbol, or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual,
- the personal opinions or views of the individual except where they relate to another individual,
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- the views or opinions of another individual about the individual, and
- the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual" (*Freedom of Information and Protection of Privacy Act*, [s.2]);

**LU ID:** means one's username and password that give access to the University's electronic systems;

**Electronic Devices:** includes but is not limited to desktops, laptops, tablet computers, cell phones, Blackberry and other personal digital assistant (PDA);

**Email:** refers to Groupwise, LU Webmail, Google Apps and any other official LU email service;

**LUNET:** means Laurentian University's intranet;

**LMS:** means Learning Management System;

**Proxy Access:** means access to the Online Library System;

**LU Wireless:** means on Campus Wireless LAN system to access the Internet and the above listed services;

**LAN system:** means the wired network;

**Webadvisor:** means the student administrative view into LU.

#### **4. Statement**

4.1 It is the policy of Laurentian University to provide quality access to its electronic systems to those who have a legitimate LU ID and visitors using Laurentian's services.

4.2 Electronic services provided by the university for the use of employees, students and other members of the university community are the property of the university, and are intended to be used in a manner that is consistent with the university's mission, standards of honest and responsible, ethical and professional conduct.

#### **5. Prohibited uses of an LU ID**

5.1 Laurentian University does not allow improper use of electronic services, including:

- a) sharing password(s);
- b) attempting to infringe on Copyright material under the Criminal Code of Canada;
- c) attempting to circumvent any security or resource management measures;
- d) generating or facilitating unsolicited commercial email ("spam"). Such activity includes, but is not limited to:
  - i. sending email in violation of the CAN-SPAM Act or any other applicable anti-spam law
  - ii. imitating or impersonating another person or his or her email address
  - iii. creating false accounts for the purpose of sending spam data
  - iv. mining any web property (to LU) to find email addresses
  - v. sending unauthorized mail via open, third-party servers
  - vi. sending emails to users who have requested to be removed from a mailing list

- e) selling, exchanging or distributing to a third party the email addresses of any person without such person's knowledge and continued consent to such disclosure;
- f) sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no pre-existing relationship;
- g) sending, uploading, distributing or disseminating or offering to do the same with respect to any unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, unlawful pornographic or otherwise objectionable content;
- h) intentionally distributing viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
- i) conducting or forwarding pyramid schemes and the like;
- j) transmitting content that may be harmful to minors;
- k) attempting to interfere with the ability of others to use the network or other commonly shared technology;
- l) impersonating another person (via the use of an email address or otherwise) or otherwise misrepresenting oneself or the source of any email and of other electronic services;
- m) illegally transmitting another's intellectual property or other proprietary information (LU and others) without such owner's or licensor's permission;
- n) attempting to discover or disclose confidential information stored on University computing facilities;
- o) using LU mail to violate the legal rights (such as rights of privacy and publicity) of others;
- p) promoting or encouraging illegal activity;
- q) interfering with other LU users' enjoyment of all LU services;
- r) creating multiple user accounts in connection with any violation of this Policy or creating user accounts by automated means or under false or fraudulent pretences;
- s) selling, trading, reselling or otherwise exploiting, for any unauthorized commercial purpose or transfer, any LU account;

- t) modifying, adapting, translating, or reverse engineering any portion of the LU services;
- u) reformatting or framing any portion of the web pages that are part of the LU service;
- v) using any LU services in connection with illegal peer-to-peer file sharing;
- w) selling, exchanging or distributing products or services for solely personal benefit and at no benefit to LU;
- x) inappropriate, offensive or pornographic use within a public areas where others can view material on the computer screen or other electronic devices and can view the person viewing the inappropriate offensive material.
- y) Any action or activity in violation of a University policy, including but not limited to the Policy on Respectful Workplace and Learning Environment and the Student Code of Conduct.

## **6. Electronic Device Protection**

- 6.1 All electronic devices with confidential information must be password protected and that all Blackberries or PDA's must have inactivity time-outs (auto-logoff).
- 6.2 The loss or theft of devices and/or unauthorized access to electronic devices and services must be reported to the University Secretariat and the Office of the Chief Information Officer immediately.

## **7. When misuse is suspected**

- 7.1 If the University reasonably suspects violation of this Policy, it is authorized to:
  - a) conduct an examination of a person or person's electronic files, programs or tape, which examination may not be limited to the physical parameters of files;
  - b) temporarily withdraw a person or person's electronic access privileges if further investigation is warranted, but only after giving notice of the suspension and after specifying a plan of investigation.

## **8. When misuse is confirmed**

8.1 If the University determines that an individual or a program initiated by an individual has deliberately violated this Policy, the University may:

- a) withdraw that person's access to the electronic facilities and resources;
- b) commence a civil action if the misuse has caused harm to the University or any member of its community, and, if criminal act or intent is suspected;
- c) contact police, who may prosecute pursuant to the Criminal Code.

## **9. University Access and Disclosure**

9.1 Laurentian University recognizes its obligation to respect confidentiality, the intellectual property and access rights of Laurentian University ID users.

9.2 Should work performed by IT for diagnostic purposes and /or maintenance require access to individual files or data that results in a violation of the confidentiality, the intellectual property or access rights, the CIO shall report the incident to the University's General Counsel or designate.

9.3 Should work performed by IT for diagnostic purposes and /or maintenance uncover information in violation of FIPPA or Human Rights, the CIO shall report the information to the University's General Counsel or designate.

9.4 Research material and intellectual property, stored on LU systems, is the property of the originator.

9.5 Except for IT diagnostic or maintenance work, access to electronic records can only be accessed when the University's General Counsel or designate declares an exceptional circumstance.

9.6 If confidential information is accessed, the individual(s) will be notified by the Privacy Officer.

## **10. Appeal Process**

10.1 To appeal the withdrawal of access (credentials), please contact Laurentian's VP Administration with subject of APPEAL.

## **11. Responsibility of all LU ID holders**

11.1 It is the responsibility of the ID holder to immediately notify the IT department of any unauthorized use of his or her password or account by someone else, by calling the IT Service Desk at x.2200 or by sending an e-mail to: [it@laurentian.ca](mailto:it@laurentian.ca).