POLICY 1.13 – Computing, Technology & Information Resources

Policy Category:	General
Subject:	Computing, Technology & Information Resources
Approving Authority:	Board of Governors
Responsible Officer(s):	President
Responsible Office(s):	Associate Vice-President (Planning, Budgeting & Information Technology), Information Technology Services
Related Procedures:	Procedures Relating to Computing, Technology & Information Resources
Effective Date:	March 15, 2017
Supersedes:	**(**NEW)

I. PURPOSE

The University's computing, technology, and information resources (hereinafter "computing resources") are allocated to individuals and groups for specific academic and administrative purposes which advance the university's mission. This policy applies to all computing, technology and information resources systems owned by and/or operated by or on behalf of the University, whether accessed through University-owned equipment or through personal devices. This policy and its accompanying procedures apply to all users of the University computing, technology and information resources, whether on campus or from remote locations, whether affiliated with the University or not, including, but not limited to:

- students
- faculty
- staff
- alumni
- contractors
- consultants
- temporary employees
- guests
- volunteers

II. DEFINITIONS

Western computing resources include all information systems, computers and computing equipment, owned by and/or operated by or on behalf of the University, as well as data owned by and/or operated by or on behalf of the University whether that data is accessed or used on University-owned equipment or on personal devices.

III. POLICY

1. Primary responsibility for security oversight and for developing rules of operation and use for all University computing systems and resources lies with the Associate Vice-President (Planning, Budgeting & Information Technology) and Information Technology Services.

2. The rights of academic freedom and freedom of expression apply to the use of University computing resources as do the responsibilities and limitations associated with those rights. The use of University computing resources is subject to the normal requirements of legal and ethical behaviour within the University community.

3. All users are required to abide by the Code of Behaviour for Use of Computing, Technology, and Information Resources which is appended to and forms part of this policy, as amended from time to time, and by such other regulations and procedures as may be put in place to protect the security of the university's computing resources. Failure to do so may result in full or partial loss of access to some or all of the University's computing resources and/or disciplinary proceedings. Further, violations of other policies, laws or terms of employment which may occur through the use of University-provided computing resources are subject to all sanctions applicable under such policies, laws or terms of employment.

4. All individuals must only use those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. The ability to access computing resources does not, by itself, imply authorization to do so.

5. The responsibility to protect University data, or information collected or used in relation to one's work, study, or voluntary activities associated with the University, extends to storage, use, or transmission of that data on personal devices.

6. All individuals must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

7. Personal use of University computing resources requires that all individuals limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. The University may require users of those computing resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will judged in the context of all of the relevant circumstances. The University is not responsible or liable for content created, sent, forwarded, contained, or stored for personal purposes.

8. Computing equipment and electronic devices provided by the University, and e-mail accounts and addresses provided by the University are the property of the University. The University reserves the right to access all University computing and information systems and records, including email records, where there are reasonable grounds to believe that those systems and/or records contain information necessary to the proper functioning of the University's

business and/or where the University is legally required to do so. Wherever practicable, affected persons will be notified promptly when their systems and/or records have been accessed.

9. The centrally administered e-mail account provided to faculty, staff, and students will be considered the individual's official university e-mail address. It is the responsibility of the account holder to ensure that e-mail received from the University at his/her official university address is attended to in a timely manner.

10. Collection, use, protection and disposal of personal or sensitive information, must be done in accordance with federal and provincial legislation and regulations, industry standards and requirements, and Western's Data Classification Procedures. Individuals should be aware that failure to comply with federal and provincial legislation may result in personal liability as well as significant consequences for Western as an institution.

11. In the event of a conflict between the provisions of this Policy or any associated Procedures and the provisions of any Collective Agreement, the provisions of the Collective Agreement shall take precedence.

12. Any breach of this Policy or any associated Procedures may be dealt with under the Code of Student Conduct in the case of a student, or the applicable Collective Agreement or other terms of employment in the case of faculty or staff. Breaches that occur as a result of individuals who are external to the University (other students or employees) will be referred to Western Legal Counsel. In the event of a breach which poses an immediate threat to the security of the University's computing resources, the Executive Director of ITS may, after consultation with the appropriate University officials, take such interim measures as he/she deems reasonably necessary to protect the security of such resources.

Code of Behaviour for Use of Computing, Information and Technology Resources

1. The University's computing resources are allocated to individuals and groups, for specific academic and administrative purposes which advance the University's mission. This Code of Behaviour applies to all users of the University's computing resources.

2. All users must ensure that the University's computing resources are used in an ethical and lawful manner. The University expects all users to conduct themselves according to the high standards of professional ethics and behaviour appropriate in an institution of higher learning.

3. As a condition of access to computing resources, a user agrees to use the computing resources solely for authorized academic, administrative purposes, and/or incidental, non-commercial personal use, and agrees to assume responsibility for any unauthorized use, misuse or illegal use of these computing resources.

4. The Unit responsible for allocating computing resources or access to corporate data to individuals and groups[1] has a responsibility to inform users about this Code. Individual users have a responsibility to read and ensure they understand this Code. The Unit shall ensure that all users receive instruction on what constitutes appropriate and inappropriate use of the facilities, and on what to do if confronted by or notified of inappropriate usage.

5. The intentional use of the computing resources for any purpose other than academic, administrative, and/or incidental, non-commercial personal use, will be considered to be unauthorized.

6. Without limiting the generality of the above, some examples of unauthorized use or misuse of computing resources are:

   (a) Using computing resources for purposes other than those for which they were allocated;

   (b) Using a computer account without authorization or providing computing resources to individuals or groups without the specific authorization of the relevant Unit Head or designate;

   (c) Inspecting, altering, deleting, obtaining copies of, publishing, or otherwise tampering with files, programs or passwords that the individual is not authorized to access;

   (d) Using computing resources for electronic communication of fraudulent, harassing or obscene messages;

   (e) Developing or using programs that harass other users or that damage the software or hardware components of the computing resources and/or placing any destructive or nuisance programs, such as viruses, in the computing resources;

   (f) Attempting to circumvent security systems on any computing resource;

[1] The unit immediately responsible for allocating such resources or access to data, e.g., an administrative work unit, Information Technology Services, Office of the Dean.

(g) Compromising or attempting to compromise the integrity of the computing resources by accessing or attempting access or alteration of system control programs or files;

(h) Using unlicensed or unauthorized copies of computer software;

(i) Breaching the terms and conditions of a software licensing agreement to which the university is a party;

(j) Theft or misappropriation of computing resources, such as equipment, data, programs or time;

(k) Engaging in any action which unfairly denies or restricts the use of computer facilities to authorized users.

7. The University may monitor the activity and accounts of individual users of university computing resources, including individual login sessions and communications, including email, without notice, under any one or more of the following circumstances:

(a) the user has voluntarily made them accessible to the public, as by posting to news groups or the web;

(b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the University from liability;

(c) there is reasonable cause to believe that the user has violated, or is violating, this policy;

(d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns

(e) it is otherwise required or permitted by law or university policy.

8. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

9. The Unit Head[2] shall ensure that a user who has been found to have been in breach of this Policy is made aware of appeal or grievance procedures available to that user.

10. Users found to have breached this Policy are subject to the full range of university disciplinary procedures, including temporary or permanent loss of access privileges, and/or legal sanctions.

[2] The Dean of a Faculty (or designate) or the Budget Head of an administrative unit (or delegate).