THE UNIVERSITY OF WINNIPEG	:

ACCEPTABLE COMPUTING USE

Purpose:

This guideline provides direction and guidance pertaining to the use of the University’s computing, information storage, software, multi-media, and network resources.

Scope:

This guideline applies to all employees, students, and other parties who access the University of Winnipeg’s information and communications technology (“ICT”) resources and facilities. This guideline applies to all ICT resources provided by, owned by, or managed by the University wherever located. It further applies to any other non-University devices connected to the University’s networks, or being used within the confines of the University.

Responsibility:

The Chief Technology Officer is responsible for the day-to-day administration of this guideline.

Definitions:

“**Custodian”** refers to individuals, groups, or departments responsible for administering computing systems, network infrastructure, and data on behalf of the University.

“CIO” refers to the most senior officer of the University charged with responsibility for the overall management of the University’s ICT resources.

“ICT” (Information and Communication Technology) refers to the computational devices, peripheral equipment, network infrastructure, and machine readable information used to capture, store, retrieve, transfer, communicate or disseminate – information through the use of electronic media.

“TSC” refers to The University of Winnipeg Technology Solutions Center.

“User” refers to any employee of the University, other academics visiting or conducting research at the University, any student enrolled at the University, guests, visitors, and authorized third parties such as contractors.

“User Identity” refers to any process, device, or mechanism (such as a logon identifier, password, account identifier, token, pass-card, etc.) that can be used to identify an individual.

Principles:

- The University of Winnipeg provides Users with ICT resources to enhance its learning environment, and to assist Users in performing their responsibilities at and for the University.
- The University accepts that its ICT assets will be used by Users for reasonable personal purposes. The privacy of individuals' electronic information shall be respected, and the University will not censor personal information on its ICT resources unless such information and use contravenes this guideline.
- Every User is bound by the responsibilities and obligations set out in this guideline and Procedures, all other University Policies and Procedures, and is subject to law. User conduct that negatively affects the University's positive learning environment, or undermines Users in any way constitutes a breach of this guideline that shall not be tolerated.
- All privately owned ICT resources that are used on University premises, or interact in any manner with University ICT resources are within the scope of this guideline. Anyone using such resources shall be subject to this guideline.

Procedures:

Distribution of Guideline

Electronic versions of this guideline shall be displayed on the University's web site.

Responsibilities of Parties

1. ***CIO*** **–** The CIO is the Custodian of the University's ICT resources. Through the CIO, TSC manages, administers, and enforces the safekeeping of these resources in accordance with University Policies, procedures, standards, and protocols.
2. ***Users*** **–** In general, Users have implicit authorization to use the ICT resources to which they have been granted access in the pursuit of their work for the University, research, and other academic pursuits. That right carries with it a responsibility to
    - use University ICT resources only for approved purposes and in compliance with all laws of Canada, a province, or international convention related to privacy of information, software licensing, trademarks, and intellectual property use;
    - comply with ICT security measures adopted by the University;
    - keep secure the User Identity provided to them since they are responsible for all activity generated using that Identity;
    - maintain and ensure the confidentiality of sensitive data;
    - report any theft, misuse, abuse, or potential threat to University ICT resources.

Unacceptable Use of Computing Resources

There are circumstances in which the use of University ICT assets would be **deemed to be unacceptable.** The following list is intended to provide guidance in determining whether an activity would contravene this guideline:

- contravening The Freedom of Information and Protection of Privacy Act (FIPPA) and similar legislation;
- attempting in any way to circumvent security measures of the University or other parties' ICT assets, services, software applications, or information;
- depriving others of access to University or other ICT resources;
- attempting to gain access to another person's User Identity without that person's explicit permission;
- downloading or disseminating licensed software, copyrighted materials, or derivative works not owned, purchased, or formally acquired by the User or the University;
- sending messages that are under false pretence, fraudulent, harassing, threatening, obscene, or perpetrating scams and hoaxes;
- mass mailing of messages or e-mail including transmitting commercial advertisements, solicitations, or promotions without prior approval of the CIO;
- using University ICT resources for personal gain and not related to the business of the University;
- deliberate alteration or destruction of computer files that the individual is not authorized to access or in contravention of retention requirements;
- failing to comply with the requirements of research granting agencies with respect to the secure storage and retention of information.

If any User is in any doubt as to the acceptability of a use of ICT resources, such person shall seek guidance from the following parties:

- in the case of employees, an immediate supervisor;
- in the case of students, the Office of the Registrar;
- in the case of matters related to academic research, the Associate Vice-President of Research;
- in the case of third parties, the CIO.

Expectation of Privacy

Under normal circumstances, Users should expect that personal information will not be accessed by other University employees. However, access may be required by University technical staff:

- in carrying out their assigned duties;

- in the course of a periodic audit of University ICT assets;
- while investigating allegations of unacceptable ICT resource use.

If in the course of these or similar activities evidence of inappropriate ICT resource use is noted, it shall be reported to the CIO. Upon direction of the CIO, TSC staff shall conduct a detailed investigation of the matter using all necessary means, including reviewing the contents of data stored on University computers or communicated using its networks.

The CIO shall report any incident to the Vice President (Academic) and Provost, or to the Vice-President (Finance and Administration) as appropriate given the role of the User. The Vice-President shall determine what action is needed:

- to end the unacceptable activity or conduct; and
- to preserve a positive learning environment; and
- to protect the University from potential liability or damage to its reputation or assets.

If required by law enforcement authorities by way of subpoena, warrant or other court order, to provide access to activity records for a specific User Identity, or specific accounts, or specific computers, the University shall comply with such lawful request in the manner required.

Consequences of Unauthorized or Unacceptable Use

Suspected violations will be investigated. Violators will have their User Identity disabled and will be subject to disciplinary procedures proscribed in;

- the Student Non-Academic Misconduct Policy; or
- University of Winnipeg Collective Agreements; or
- relevant Policies, procedures or protocols then in effect.

In cases of financial loss to the University, the University may seek restitution. In severe cases, or where required by law, the matter shall be referred to the appropriate law enforcement agency.

Incident Reporting

Users are strongly urged to report to the TSC Service Desk any incidents of unacceptable use that they observe. Incidents will be handled in accordance with processes outlined in the IT Resource Incident Response Protocol.