

**POLICY TITLE:** University of Guelph Acceptable Use Policy for Information Technology

**Policy #:** CIO-ITSecurity-03.1.3  
**Initial Draft By:** Position / Date: AUP Review Committee – April 30, 2012  
**Circulation Draft By:** Position / Date: IT Security Officer – July 23, 2012  
**Final Draft By:** Position / Date: Dir. ITPMO – December 3, 2012  
**APPROVED BY / DATE:** Position / Date: **CIO – December 3, 2012**  
**Last Revised Date:** December 3, 2012  
**Next Review Date:** One year after Approval

**BRIEF DESCRIPTION:** This document defines acceptable use and breaches of acceptable use of Information Technology Resources at the University of Guelph.

## University of Guelph Acceptable Use Policy for Information Technology

### 1. Purpose and Jurisdiction

The purpose of this policy is to define the acceptable use of Information Technology (IT) Resources in support of the mission of the University of Guelph. It builds on the principles of accountability, transparency, privacy, and fairness, to support a functional environment for work and study in which these resources are protected. This policy applies to anyone who uses or accesses any IT Resource belonging to, under the control or in the custody of, the University of Guelph.

### 2. Definitions

For the purposes of this policy, the following terms are defined as follows:

**Account** – includes any username, access code, password, PIN, token, credential, or other authentication which has been assigned to Authorized Users to use any University IT Resource.

**Authorized** – means specific access rights granted in accordance with University governance or policies.

**Authorized User** – means a member of the University of Guelph community, who is an employee, student, alumni, associate, or other individual who has been granted specific rights by a University signing officer, or someone delegated in accordance with University governance or policies to use any University IT Resource.

**Community Standards** – means behaviour or material which the average member of the University Community would reasonably tolerate.

**Information Technology (IT) Resource** – means any information, data, software, hardware, system, or network belonging to, under the control or in the custody of the University, regardless of who administers it.

**Information Technology (IT) Security Officer** – means the University employee or designate who is responsible for enforcing the Acceptable Use Policy

**Personal Information** – means recorded information about an identifiable individual, and as defined in federal and provincial privacy legislation

**System Administrator** – means an individual responsible and authorized to establish or maintain and provide technical support for a University IT Resource.

### **3. Acceptable Use**

The University of Guelph authorizes the University community to use its Information Technology Resources to fulfill and advance the University's teaching, learning, research, service, administrative, and community development missions.

In addition, the University permits limited personal use of these resources, provided this use does not violate any law, statute, or University policy. Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the University's IT network.

The University respects the privacy of all users of its IT Resources, and uses reasonable efforts to maintain confidentiality of Personal Information. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to:

1. Access to Personal Information may be granted to an Authorized User, System Administrator or agent to meet legitimate University business needs and operational requirements, or in the event that an Authorized User is unavailable, or has his or her access revoked.
2. The University may audit, access or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Such access will be subject to the authorization of the appropriate Vice-President (or designate) in consultation with the Provost.

Authorized Users must exercise good judgment in determining what is acceptable use of IT Resources with due regard to this policy, other University policies and Community Standards. Some activities may be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context.

Authorized Users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT Resources and report encountered vulnerabilities to the Information Technology Security Officer. Failure to do so may constitute a breach of this policy.

## **Examples of a Breach of Acceptable Use**

**Unless explicitly authorized**, a breach of acceptable use includes, but is not limited to:

1. Allowing others to access your assigned personal Account
2. Failure to exercise reasonable care in safeguarding Accounts and information
3. Accessing someone else's personal Account
4. Seeking information on passwords or information belonging to others
5. Breaking or attempting to circumvent licensing or copyright provisions
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information
7. Attempting to collect, use, or disclose, the Personal Information of others
8. Using IT resources to harass or bully others
9. Attempting to circumvent information security provisions or exploit vulnerabilities
10. Using IT Resources (e.g. University computing account or workstation) for unauthorized commercial purposes
11. Any interference with the ability of others to use IT Resources whether it is disruptive or not
12. Falsifying or misrepresenting your identity
13. Viewing or using pornographic or offensive material in a work, study, or public location
14. Distributing or disseminating pornographic or offensive material in any location

## 4. Outcomes

If the integrity or security of an IT Resource is compromised or at risk the Information Technology (IT) Security Officer may direct the locking or quarantining of an Account or resource at his or her sole discretion. Upon reasonable belief by the IT Security Officer that a violation of this policy (AUP) may have occurred, the IT Security Officer or designate will conduct an investigation.

If access to any Personal Information is required, authorization will be requested of the appropriate Vice-President (or designate) in consultation with the Provost.

If insufficient evidence of a violation of the AUP is found, the investigation will be closed and involved parties notified where appropriate.

The IT Security Officer will issue a written decision regarding the alleged policy violation within a reasonable timeframe, normally 30 days. Actions noted below may be initiated upon determination of a violation of this policy.

An Authorized User affected by this decision may file an appeal to the Chief Information Officer (CIO). The Authorized User will have 10 calendar days from the issuance of a written decision to file an appeal with the CIO. The CIO may confirm, rescind, or modify the decision. The decision of the CIO is considered final.

If a violation is determined to have occurred, the following actions may be initiated by the IT Security Officer:

<b>Class or severity</b>	<b>Possible outcomes</b>
Minor violation of the AUP	Warning
Serious or repeated violation of the AUP	Escalation to appropriate authority or disciplinary process and/or restrictions on access or use
Possible violation of another University policy or regulation	Forward for investigation by applicable process under the applicable policy or regulation
Possible violation of federal, provincial, or municipal law or statute	Forward for investigation to Campus Community Police

## **5. Related University Policies**

This Acceptable Use Policy prohibits any use of IT Resources which potentially violates any other University of Guelph policy, code or agreement, constitutes academic or non-academic misconduct, or which violates federal, provincial, or municipal laws or regulations.

In addition to outcomes under the AUP, such violations may be prosecuted under those laws and policies. Any information resulting from an investigation under the AUP may be shared for the purposes of such prosecutions.

Some of these policies include:

- Human Rights Policy
- Graphics Standards Guide
- Mass Electronic Mail Policy
- Protection of Privacy and Access to Information
- Release of Student Information
- Residence Community Living Standards
- Student Rights and Responsibilities
- University Undergraduate or Graduate Calendars
- Human Resources Policies
- Collective Agreements or other Employment Agreements

A more comprehensive list of applicable University policies is maintained by the University Secretariat at <http://www.uoguelph.ca/policies/>.

## **6. Departmental AUPs**

Departments may have Departmental Acceptable Use Policies to meet their specific operational requirements. An Authorized User using Departmental IT Resources is bound by the Departmental AUP. In the event of a conflict between the Departmental AUP and this policy, this policy prevails.

Essential Components of Departmental AUPs are:

1. A copy of the Departmental AUP must be available to all employees of that department
2. Definition or description of Departmental IT Resources which the Departmental AUP applies to
3. One or more locations where the current University and departmental AUPs may be found.
4. List of user responsibilities and expectations specific to the use of Departmental IT Resources with clear examples of unacceptable actions of activities

5. An indication of actions and examinations considered routine with regard to Departmental IT Resources
6. How suspected violations of the Departmental AUP are handled
  - a. Department Chair for violations specific to the Departmental AUP
  - b. IT Security Officer for issues related to the University AUP
7. The circumstances under which accounts or access to Departmental IT Resources is terminated or restricted

Any Departmental AUP will be submitted for review to the Chief Information Officer or designate prior to implementation. Review will be completed within a reasonable timeframe, normally 30 days.

### **Change/Approval History**

- Approved (after final editing @ ITSC) – December 3, 2012
- Final Draft (initial) – November 13, 2012 – D. D. Badger, Dir. PMO
- Circulation Draft – July 23, 2012 – G. Bos, IT Security Officer
- Approval for Circulation – July 10, 2012 – CIO/ Information Technology Strategy Committee
- Creation of Initial Draft – Apr 30, 2012 – AUP Review Committee (G. Bos, Chair)