Approval Date: June 25, 2010

Information Technology Use and Management Policy

Office of Accountability:	Provost and Vice-President (Academic) Vice President (Finance and Administration)
Office of Administrative Responsibility:	Vice-Provost and Associate Vice-President (Information Technology)
Approver:	Board of Governors
Scope:	Compliance with University procedure extends to all members of the University community.

Overview

The University of Alberta strives to foster and maintain an intellectual environment in which **members of the University community** can access and create **information**, and collaborate with colleagues and peers. As part of this effort, the University is committed to maintaining an information technology environment that is free from harassment and is accessible to its members.

Such an environment can only exist when all members use and manage the **information technology resources** responsibly, respectfully and in a manner that reflects high ethical standards, mutual respect and civility.

Use of the University of Alberta's information technology resources must comply with all applicable laws, University of Alberta policies, procedures, appendices and guidelines.

Purpose

The purpose of this policy is to define the University's expectations and requirements to the use and management of University information technology resources.

POLICY

1. University information technology resources are to be used primarily for activities related to the mission of the University, including, but not limited to teaching, learning, research and administration. Limited personal use (i.e. use not related to the mission of the University) is permitted provided it complies with this Policy, does not compromise the business of the University, does not increase the University's costs, does not expose the University to additional risk, does not damage the University's reputation, and does not unduly impact the University's business and academic uses. All other uses are prohibited.

2. Information Technology resources must be used and managed in a responsible manner. Use of these resources for disruptive, fraudulent, harassing, threatening, obscene (including but not limited to racist, profane, and pornographic in nature), or malicious purposes is strictly prohibited. Use of information technology resources for commercial purposes is prohibited unless authorized by the appropriate Dean or Director.

3. Application and enforcement of this policy shall not in any way, constrain academic freedom on campus.

4. Use of University information technology resources, including **electronic identities**, is permitted only to members of the University community, and **authorized guests**. Requests for authorized guest use, must follow the CCID enrollment process, unless the resource requested is in the public domain, such as the library catalogue system or public websites. Unless otherwise stated, such access, including the use of electronic identities, is authorized only on an individual basis and may not be shared by multiple individuals. Anyone granted authorization to use an electronic identity must make all reasonable efforts to keep such identification private and secure.

5. Information technology resource users must stay within their authorized limits and refrain from seeking to gain unauthorized access to information technology resources beyond their permissions and privileges.

6. Any individual using information technology resources to create, access, transmit or receive University-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

7. Users must respect the rights of other users. They must not encroach on other users' rights to use, access, and privacy.

8. All forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. Users must refrain from transmitting to others, inappropriate images, sounds, or messages which might reasonably be considered harassing, fraudulent, threatening, obscene (e.g. pornographic), defamatory, or other messages or material that are a violation of applicable law or University policy.

9. Users must be sensitive to the open nature of public spaces (for example, computer labs and classrooms) and take care not to display in such locations images, sounds or messages that are harassing, threatening, obscene (e.g. pornographic), defamatory, or that are a violation of applicable law or University policy.

10. Users must respect intellectual property, copyrights, and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

11. The University will protect information against unauthorized disclosure. The University reserves the right to access, monitor and record both stored or in-transit data and the usage of information technology resources when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the *Freedom of Information and Protection of Privacy Act*, or as otherwise required by law. The University has the right to use information gained in this way in disciplinary actions as prescribed in University policies, and to provide such information to appropriate internal and external investigative authorities.

12. Anyone witnessing or suspecting an information technology security incident and/or unacceptable use of University information technology resources in a manner that contravenes this Policy, is obligated to respond and report in accordance to the Responding to and Reporting of Information Security Breaches Procedure.

Support and assistance can be obtained from IST at 780-492-9400 | ist@ualberta.ca.

Assistance from the Office of the Chief Information Security Officer (CISO) is available through ciso@ualberta.ca.

13. The University reserves the right to withhold and revoke access to its information technology resources to any individual if there are reasonable grounds to suspect that their continued access to the resources poses a threat to the operation of the resource or the reputation of the University.

14. The University's actions under this policy will be taken in accordance with the *Ethical Conduct and Safe Disclosure Policy*.

15. **System administrators** of information technology resources have the responsibility to investigate and take action in the case of suspected or alleged unacceptable use. With the approval of their supervisor and with due regard for the rights of users' privacy and the confidentiality of users' data, system administrators have the right to suspend or modify users' access privileges to information technology resources. System administrators have the responsibility to take immediate action in the event the University is at imminent risk. System administrators may examine files, passwords, accounting information, data, and any other material that may aid in an investigation of possible abuse.

16. Non-compliance with this policy constitutes misconduct and may be handled under the applicable collective agreements, University policy, or law.

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. **[▲ Top]**

Members of the University Community	University staff, faculty, students, and other holders of valid CCID.
Information	Data, or aggregate data, created using University information technology resources.
Information technology resources	Information technology resources refer to all hardware, software, and supporting infrastructure owned by, or under the Custodianship of, the University that is used to create, retrieve, manipulate, transfer and store electronic information. This includes (but is not limited to), central and non-centrally supported computers, file systems attached to these computers, operating systems running on these computers, software packages supported by these operating systems, wired and wireless networks, telecommunication and hand-held devices, data stored on or in transit on the above, as well as electronic identities used to identify and authenticate the users of the aforementioned resources.
Electronic identity	An electronic identity is any means by which a person may be identified and authenticated to access an information technology resource. This includes, but is not limited to, an account name and password, encryption keys, proximity cards, swipe cards, smart cards, or other forms of identification.
Authorized guests	Other authorized users of information technology resources may include, but are not limited to, conference attendees, prospective students, and users of University public domain resources.
Information Technology Security Incident	Events where there is suspicion that: • the confidentiality, integrity, and availability of University data has been compromised • information and information technology resources are used for, or violated by, illegal or criminal activity • information technology resources has been attacked, is currently under attack, or is vulnerable to attack.
System administrator	System administrator refers to the person or persons responsible for configuring, installing, maintaining, and supporting information technology resources for a faculty, department, and unit. A system administrator of an information technology resource may also be a user of that resource.

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. **[▲ Top]**

Access to Information and Protection of Privacy Policy (UAPPOL)

Information Services and Technology (IST) (University of Alberta)

Code of Student Behavior (University of Alberta)

Copyright Act (Department of Justice)

Ethical Conduct and Safe Disclosure Policy (UAPPOL)

Freedom of Information and Privacy Protection Act (Government of Alberta)

PUBLISHED PROCEDURES OF THIS POLICY

Information Technology Use and Management Policy (Appendix A) Examples of Unacceptable Use (UAPPOL)

Responding to and Reporting of Information Security Breaches Procedure (UAPPOL)