ACADIA UNIVERSITY

POLICIES and PROCEDURES

Responsible Unit	Computing Services
Policy Number	T-1
Date Last Updated	01 November 2013
Approving Sector Head	Vice-President, Academic
Policy	**TECHNOLOGY SERVICES**

These policies are intended to promote the responsible and ethical use of University computer resources. The resources should be used for the purposes for which access is granted, according to practices which ensure that the rights of all users are protected. A “user” is defined as any students, staff or faculty member with authorized access to any computer system at Acadia. Any employee with a demonstrable work-related need for computer access, and who has departmental authorization, is entitled to a computer account.

Note: These policies are reviewed periodically. Please be advised that these policies may change. Watch for system messages, posters, etc.

Certain activities by users constitute abuse. Computer abusers are liable for monetary payment of their abuse, restriction or curtailment of computing privileges, and may be subject to further discipline by the University. In some cases they may be liable for civil or criminal prosecution. Complaints against students regarding violation of computing policies are handled through the Office of Student Services and follow the judicial procedures outlined in the Student Handbook. Complaints against other users regarding violation of computing policies are handled by the unit responsible for the individual against whom the complaint was made and/or the unit responsible for the location where the action giving rise to the complaint occurred. Appeals concerning the imposition of any penalty may be made to the appropriate Director and then to the Senior Administrator responsible for that Director. These policies govern the use of all of Acadia’s computing facilities including terminals, microcomputers, mini-computers, mainframes or network facilities which are the property of Acadia University.

Acadia University has established the following general principles:

- The use of University computing and networking facilities requires authorization and is for University use only.
- Attempting to discover or disclose confidential information stored on University computing facilities is not permitted.
- The University abides by the terms of the licensing agreements it has entered into for computer software and equipment facilities.
- University-related work takes priority.
- The University does not permit the use of its computing and networking facilities for illegal activities or harassment.

- The use of University computing and networking facilities complies with University operational policies and procedures.
- Breaking Acadia University published policies constitutes a breach of employment conditions and/or academic integrity.
- Permission to access data in another user's account must be authorized in writing by that user, or where this is not possible, by the appropriate Senior Administrator.
- Users are responsible for activities originating on computer equipment and/or network connections assigned to them.
- It is an offence to break any computing policies set by the University.

As with all matters of law and ethics, ignorance of the rules does not excuse violations. Note that without prior written authorization by the President, it is contrary to University policies for any user to:

- permit another person to log in to your account (your account passwords are confidential and under no circumstances should they be distributed)
- log in to another person's account, even if you have permission
- attempt to discover another user's password
- copy, disclose, or transfer any of the computer software provided by Acadia University without written permission from the department that acquired or licensed it
- use any Acadia University computer/network equipment or software to violate the terms of any software License Agreement
- attempt to bypass standard procedures (This includes, but is not limited to, circumventing standard disconnect functions for dial-in lines, unauthorized use of a password and accessing a file without permission. Accessing a file refers to copying, reading, renaming, changing or deleting. Lack of file protection does not give you the right to do any of these things.)
- use University computing/network facilities for personal profit-making activities
- exceed any posted time limit on a terminal or microcomputer when others are waiting
- use University network facilities to send nuisance, abusive, obscene, forged or anonymous messages to anyone within the University community or externally
- use University network facilities to harass other users
- change the name assigned to an account
- tamper with University computing/network equipment such as microcomputers, printers, or network jacks (problems should be reported to the appropriate department
- collect or discard output other than your own without the owner's permission
- violate any of the "LAB RULES" posted in the public microcomputer facilities
- use the University network facilities to provide computing services outside the University's network, without authorization from the Technology Services department
- use the University network facilities to provide any external computing service to the campus community, without authorization from the Technology Services department.

Software

The use of software on the Acadia University computers is governed by the terms of License Agreements between Acadia University and software vendors. These software programs are of a proprietary nature and/or may contain trade secrets or be subject to a copyright or patent as defined in License Agreements. All users of software acquired by Acadia University must abide by the terms of these license Agreements. Link to: *Microsoft Licensing Product Use Rights*

The following actions are considered illegal and may subject the perpetrator to sanctions by the University:

- Providing copies of copyrighted or licensed software to others while maintaining copies for one's own use, unless there is a specific provision in the license which allows such activity. The activity is forbidden even if the software is provided without cost for an educational purpose.
- Using software or documentation known to have been obtained in violation of the Copyright Law or a valid license provision. Use of a copy of a copyrighted program obtained from another party for which no license exists that allows for such a transfer will be presumed to be knowing, and the burden of demonstrating that the use was innocent will rest with the user.
- Using a copyrighted program on more than one machine at the same time, unless a specific license provision permits such activity.
- Copying any copyrighted printed documentation. Violation of any of these policies is considered an abuse of that privilege granted, and may lead to the withdrawal of an account and/or other disciplinary action.

<u>Administrative Policies</u>

- The Technology Services Systems Support Group has the responsibility for keeping systems working and to protect the confidentiality of a user's work. This confidentiality will be respected until there is an indication that the user has become part of something that has caused a problem with the operations of systems or the confidentiality of another user's work.
    - A request to access data in another user's account must be authorized in writing by the user, or where this is not possible, by the appropriate Senior Administrator.
    - Technology Services reserves the right to view and/or delete user files without prior notice or written authorization when the stability, integrity and/or the security of the system is being threatened by actions on the part of that user.
    - Technology Services also has the right to terminate any process when deemed necessary, in order to maintain the system.
    - It should be noted that abusers are normally identified by their user names. Users who allow others to use their accounts may find themselves restricted and/or disciplined if others abuse the system with their name.
    - When in doubt, it is best to do only what you have been specifically permitted to do, e.g., if you have permission to use a program or file, do not make a copy (even on paper) unless you have been explicitly told you may do so.

- The use of University computing and network facilities to solicit credit card information requires authorization from Technology Services.

<u>Computer Accounts</u>

The following governs the authorization and creation of network login accounts and electronic mail accounts. Access to specific data or software applications falls outside the scope of this policy, and is authorized by the data/application owner, or in the case of administrative systems, by the appropriate data steward(s). Technology Services has the right to disable any account after having reasonable evidence that any computing policy has been violated.

- Students
    - A computer account and e-mail account are created for each new student at the start of the academic year, and remain valid until September 30th of the following year. After each fall registration and prior to the expiry date, Novell and e-mail accounts for all registered students (as well as accounts on the academic Unix server for registered BCS students) are automatically extended for another year, without any additional action by the student. As a

    security measure, student account passwords expire annually, and require resetting by the account owner. Any student withdrawing from Acadia will have his/her account(s) disabled immediately, and such account(s) will be deleted from disk after two weeks.
    - Graduates since May 2000 are entitled to retain their Acadia e-mail address.

- Faculty/Staff (excluding sessional)
    - Any employee with a demonstrated work-related need for computer access, and who has departmental authorization, is entitled to a computer account. Employment is confirmed through the Human Resources Department.
    - Faculty and staff computer accounts are active only during the period of employment. Accounts are disabled when the employee leaves Acadia, and are removed from disk after 30 days.
    - Upon retiring, full-time faculty and staff are entitled to retain an Acadia e-mail address.

- Sessional Employees
    - Any sessional employee with a demonstrable work-related need for computer access, and who has departmental authorization, is entitled to a computer account. Employment is confirmed through the Human Resources Department.
    - Professors on multi-year contractually limited term contracts, having appointments each of at least nine (9) months duration, will retain their computer account and e-mail access during the summer break.
    - Accounts for other sessional appointments are active only during the period of the session. They are removed from disk two weeks after the start of the next session, unless the employee has returned and the account has been renewed. Similarly, these sessional employees do not have access to their Acadia electronic mail beyond the sessional period. Before leaving at the end of a session, they may place an “Out of Office” message on the e-mail account, or forward incoming messages to another Acadia staff e-mail address during their absence.

- Guest Accounts
    - A guest account and/or Acadia e-mail address may be required for a person who is affiliated with Acadia but who is not defined as a regular employee on the payroll, nor as an active student. This includes volunteers, external consultants, visiting scholars, and affiliated committee members (e.g., Senate, Board of Governors).
    - A guest account must be authorized by the appropriate Dean or Senior Administrator, and is available for periods of up to one year as required. A guest account may be renewed beyond one year by submitting a new request.
    - If not renewed, a guest account id disabled at the end of the account term, and is removed from disk after 30 days.

- Exceptions
    - In exceptional circumstances, the Director of Technology services can authorize computer account access for a brief period.

Wireless Networks

This governs the use of any devices that operate on the 2.4GHz radio frequency on Acadia’s campus. These devices are not limited to IEEE 802.11 wireless networking devices, but could also include equipment such as cordless phones, microwave ovens, and audio speakers.

The use of some types of wireless equipment can cause network interference or introduce serious security problems. In order to ensure the highest level of service to the users of Acadia's wireless network, all members of the campus community are asked to minimize the potential for such interference.

In cases where specialized wireless equipment is being used for teaching or research applications, Technology Services will work with the individual to determine whether there are circumstances under which use of the equipment can be accommodated without causing interference to Acadia's wireless users. Technology Services does not actively monitor the airspace for potential interfering devices, but does randomly check for unauthorized network devices that could compromise network security.

Guidelines:

- Wireless networking is an extension of Acadia's campus network, and required authorization by Senior Administration.
- In order to ensure a high-quality, supportable and secure network infrastructure, all wireless access points at Acadia are to be installed, configured and managed by Technology Services personnel.
- All access to Acadia's wireless network must be authorized and authenticated with a valid Acadia login and password and must meet Acadia's wireless network standards.
- Devices that interfere with the normal operation of the University's wireless network will not be allowed on campus. The University reserves the right to see out the user of such devices if there is evidence of interference, disruption to the network or breaches of security, and to remove the device if network problems cannot be corrected.
- The University reserves the right to remove any unauthorized access points installed on Acadia property.