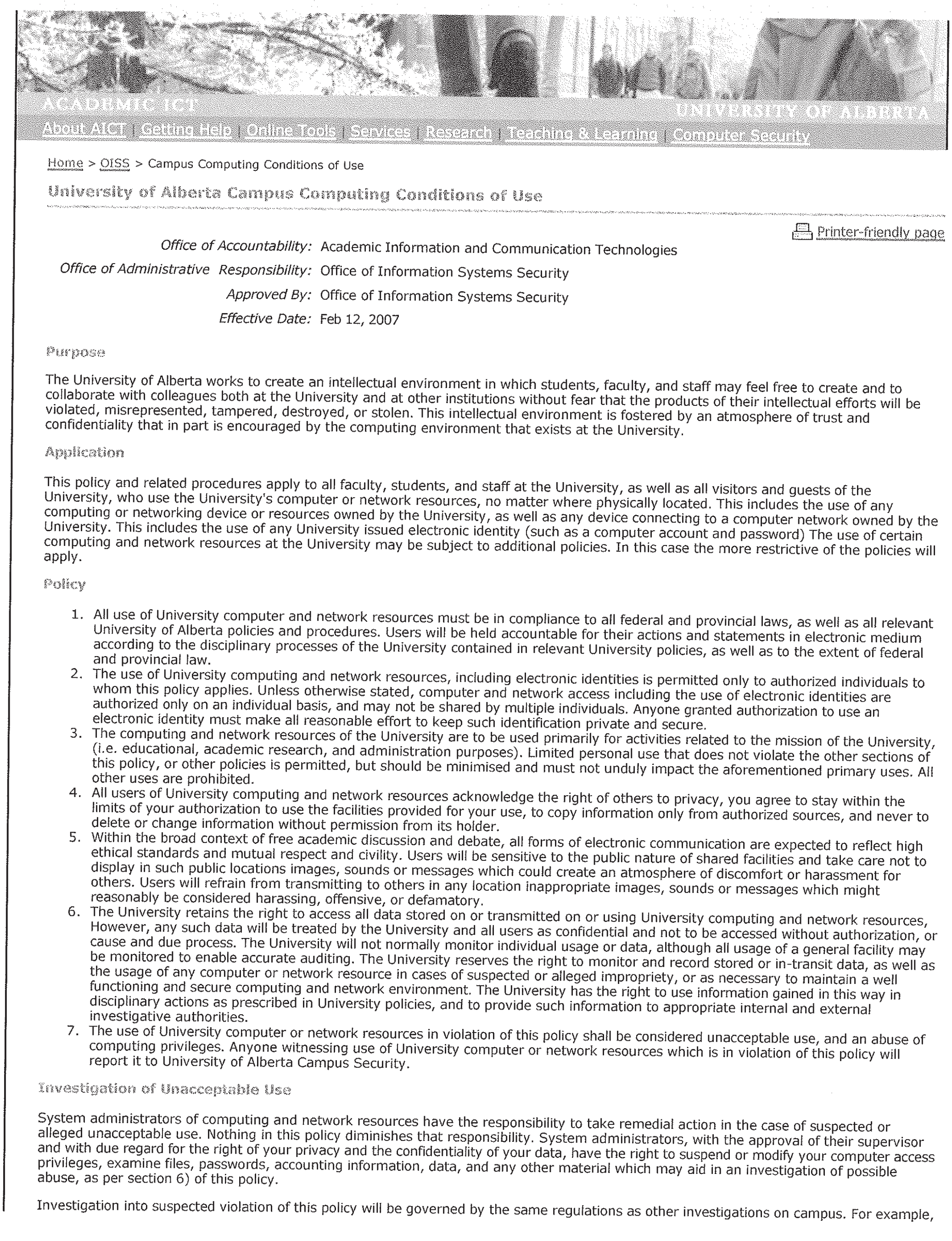
Public Computing Policies

UNIVERSITY OF ALBERTA

http://www.ualberta.ca/AICT/OISS/policies/conditionsofuse.htm


ACADEMIC ICT
UNIVERSITY OF ALBERTA
About AICT | Getting Help | Online Tools | Services | Research | Teaching & Learning | Computer Security

Home > OISS > Campus Computing Conditions of Use

University of Alberta Campus Computing Conditions of Use

Printer-friendly page

Office of Accountability: Academic Information and Communication Technologies
Office of Administrative Responsibility: Office of Information Systems Security
Approved By: Office of Information Systems Security
Effective Date: Feb 12, 2007

Purpose

The University of Alberta works to create an intellectual environment in which students, faculty, and staff may feel free to create and to collaborate with colleagues both at the University and at other institutions without fear that the products of their intellectual efforts will be violated, misrepresented, tampered, destroyed, or stolen. This intellectual environment is fostered by an atmosphere of trust and confidentiality that in part is encouraged by the computing environment that exists at the University.

Application

This policy and related procedures apply to all faculty, students, and staff at the University, as well as all visitors and guests of the University, who use the University's computer or network resources, no matter where physically located. This includes the use of any computing or networking device or resources owned by the University, as well as any device connecting to a computer network owned by the University. This includes the use of any University issued electronic identity (such as a computer account and password) The use of certain computing and network resources at the University may be subject to additional policies. In this case the more restrictive of the policies will apply.

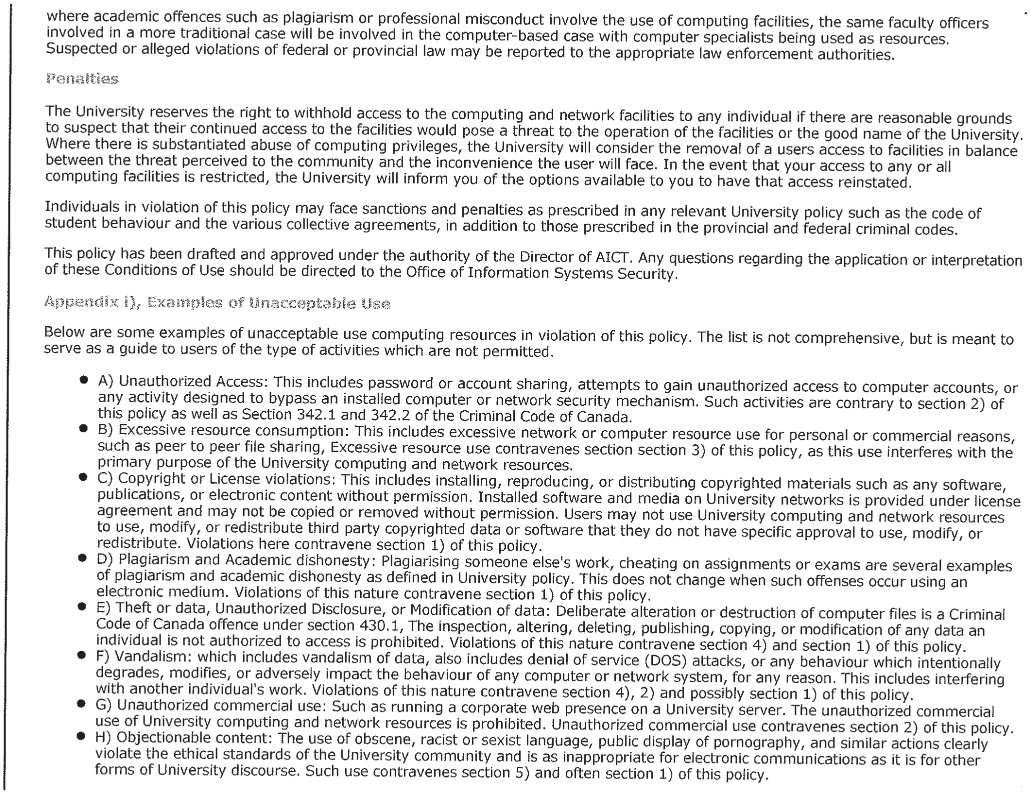
Policy

1. All use of University computer and network resources must be in compliance to all federal and provincial laws, as well as all relevant University of Alberta policies and procedures. Users will be held accountable for their actions and statements in electronic medium according to the disciplinary processes of the University contained in relevant University policies, as well as to the extent of federal and provincial law.
2. The use of University computing and network resources, including electronic identities is permitted only to authorized individuals to whom this policy applies. Unless otherwise stated, computer and network access including the use of electronic identities are 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 effort to keep such identification private and secure.
3. The computing and network resources of the University are to be used primarily for activities related to the mission of the University, (i.e. educational, academic research, and administration purposes). Limited personal use that does not violate the other sections of this policy, or other policies is permitted, but should be minimised and must not unduly impact the aforementioned primary uses. All other uses are prohibited.
4. All users of University computing and network resources acknowledge the right of others to privacy, you agree to stay within the limits of your authorization to use the facilities provided for your use, to copy information only from authorized sources, and never to delete or change information without permission from its holder.
5. Within the broad context of free academic discussion and debate, all forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. Users will be sensitive to the public nature of shared facilities and take care not to display in such public locations images, sounds or messages which could create an atmosphere of discomfort or harassment for others. Users will refrain from transmitting to others in any location inappropriate images, sounds or messages which might reasonably be considered harassing, offensive, or defamatory.
6. The University retains the right to access all data stored on or transmitted on or using University computing and network resources, However, any such data will be treated by the University and all users as confidential and not to be accessed without authorization, or cause and due process. The University will not normally monitor individual usage or data, although all usage of a general facility may be monitored to enable accurate auditing. The University reserves the right to monitor and record stored or in-transit data, as well as the usage of any computer or network resource in cases of suspected or alleged impropriety, or as necessary to maintain a well functioning and secure computing and network environment. 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.
7. The use of University computer or network resources in violation of this policy shall be considered unacceptable use, and an abuse of computing privileges. Anyone witnessing use of University computer or network resources which is in violation of this policy will report it to University of Alberta Campus Security.

Investigation of Unacceptable Use

System administrators of computing and network resources have the responsibility to take remedial action in the case of suspected or alleged unacceptable use. Nothing in this policy diminishes that responsibility. System administrators, with the approval of their supervisor and with due regard for the right of your privacy and the confidentiality of your data, have the right to suspend or modify your computer access privileges, examine files, passwords, accounting information, data, and any other material which may aid in an investigation of possible abuse, as per section 6) of this policy.

Investigation into suspected violation of this policy will be governed by the same regulations as other investigations on campus. For example, http://www.ualberta.ca/AICT/OISS/policies/conditionsofuse.htm



where academic offences such as plagiarism or professional misconduct involve the use of computing facilities, the same faculty officers involved in a more traditional case will be involved in the computer-based case with computer specialists being used as resources. Suspected or alleged violations of federal or provincial law may be reported to the appropriate law enforcement authorities.

Penalties

The University reserves the right to withhold access to the computing and network facilities to any individual if there are reasonable grounds to suspect that their continued access to the facilities would pose a threat to the operation of the facilities or the good name of the University. Where there is substantiated abuse of computing privileges, the University will consider the removal of a users access to facilities in balance between the threat perceived to the community and the inconvenience the user will face. In the event that your access to any or all computing facilities is restricted, the University will inform you of the options available to you to have that access reinstated.

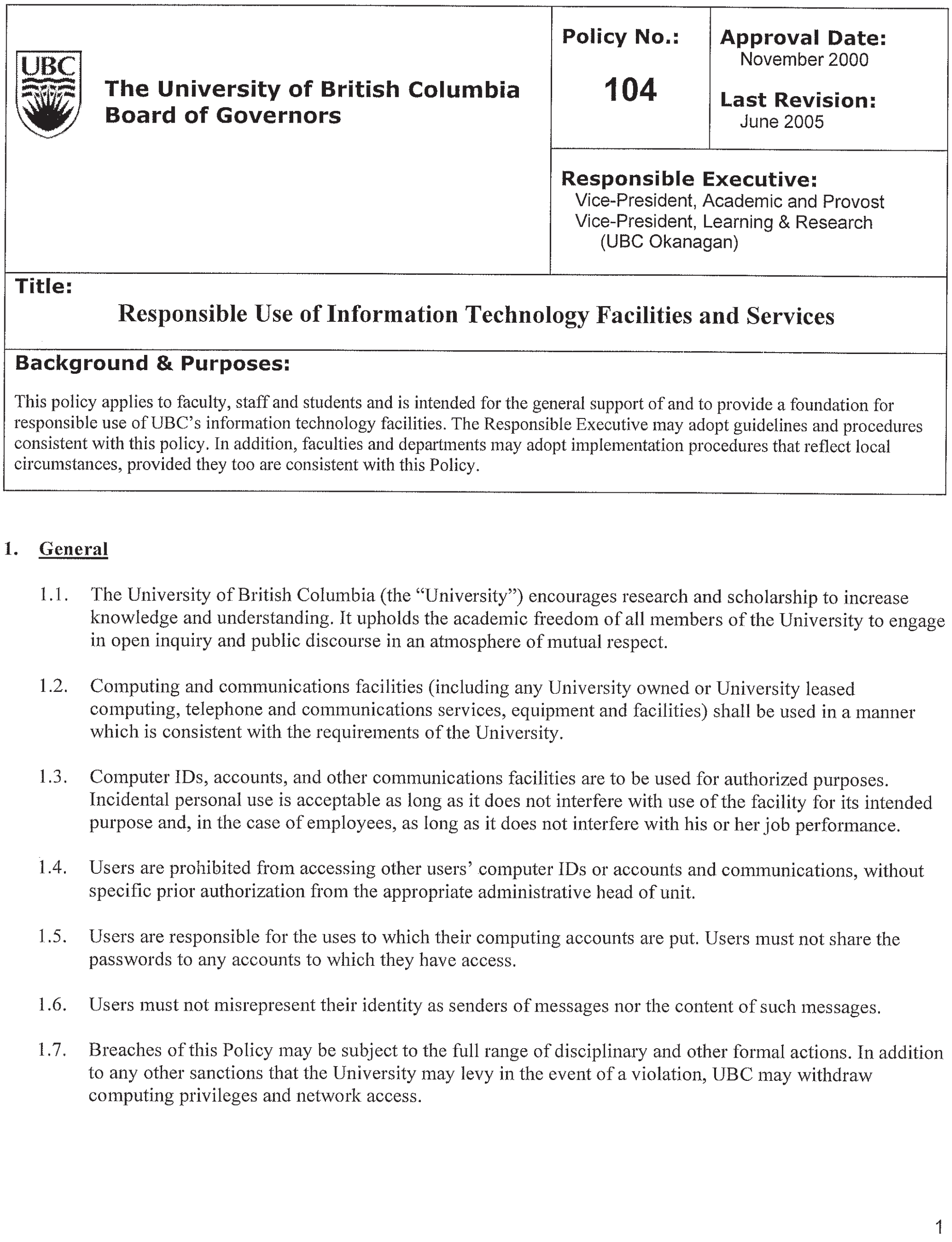
Individuals in violation of this policy may face sanctions and penalties as prescribed in any relevant University policy such as the code of student behaviour and the various collective agreements, in addition to those prescribed in the provincial and federal criminal codes.

This policy has been drafted and approved under the authority of the Director of AICT. Any questions regarding the application or interpretation of these Conditions of Use should be directed to the Office of Information Systems Security.

Appendix i), Examples of Unacceptable Use

Below are some examples of unacceptable use computing resources in violation of this policy. The list is not comprehensive, but is meant to serve as a guide to users of the type of activities which are not permitted.

- A) Unauthorized Access: This includes password or account sharing, attempts to gain unauthorized access to computer accounts, or any activity designed to bypass an installed computer or network security mechanism. Such activities are contrary to section 2) of this policy as well as Section 342.1 and 342.2 of the Criminal Code of Canada.
- B) Excessive resource consumption: This includes excessive network or computer resource use for personal or commercial reasons, such as peer to peer file sharing, Excessive resource use contravenes section section 3) of this policy, as this use interferes with the primary purpose of the University computing and network resources.
- C) Copyright or License violations: This includes installing, reproducing, or distributing copyrighted materials such as any software, publications, or electronic content without permission. Installed software and media on University networks is provided under license agreement and may not be copied or removed without permission. Users may not use University computing and network resources to use, modify, or redistribute third party copyrighted data or software that they do not have specific approval to use, modify, or redistribute. Violations here contravene section 1) of this policy.
- D) Plagiarism and Academic dishonesty: Plagiarising someone else's work, cheating on assignments or exams are several examples of plagiarism and academic dishonesty as defined in University policy. This does not change when such offenses occur using an electronic medium. Violations of this nature contravene section 1) of this policy.
- E) Theft or data, Unauthorized Disclosure, or Modification of data: Deliberate alteration or destruction of computer files is a Criminal Code of Canada offence under section 430.1, The inspection, altering, deleting, publishing, copying, or modification of any data an individual is not authorized to access is prohibited. Violations of this nature contravene section 4) and section 1) of this policy.
- F) Vandalism: which includes vandalism of data, also includes denial of service (DOS) attacks, or any behaviour which intentionally degrades, modifies, or adversely impact the behaviour of any computer or network system, for any reason. This includes interfering with another individual's work. Violations of this nature contravene section 4), 2) and possibly section 1) of this policy.
- G) Unauthorized commercial use: Such as running a corporate web presence on a University server. The unauthorized commercial use of University computing and network resources is prohibited. Unauthorized commercial use contravenes section 2) of this policy.
- H) Objectionable content: The use of obscene, racist or sexist language, public display of pornography, and similar actions clearly violate the ethical standards of the University community and is as inappropriate for electronic communications as it is for other forms of University discourse. Such use contravenes section 5) and often section 1) of this policy.



The University of British Columbia Board of Governors	**Policy No.:** 104	**Approval Date:** November 2000 **Last Revision:** June 2005
	Responsible Executive: Vice-President, Academic and Provost Vice-President, Learning & Research (UBC Okanagan)	

Title:

Responsible Use of Information Technology Facilities and Services

Background & Purposes:

This policy applies to faculty, staff and students and is intended for the general support of and to provide a foundation for responsible use of UBC's information technology facilities. The Responsible Executive may adopt guidelines and procedures consistent with this policy. In addition, faculties and departments may adopt implementation procedures that reflect local circumstances, provided they too are consistent with this Policy.

1. General

1.1. The University of British Columbia (the "University") encourages research and scholarship to increase knowledge and understanding. It upholds the academic freedom of all members of the University to engage in open inquiry and public discourse in an atmosphere of mutual respect.

1.2. Computing and communications facilities (including any University owned or University leased computing, telephone and communications services, equipment and facilities) shall be used in a manner which is consistent with the requirements of the University.

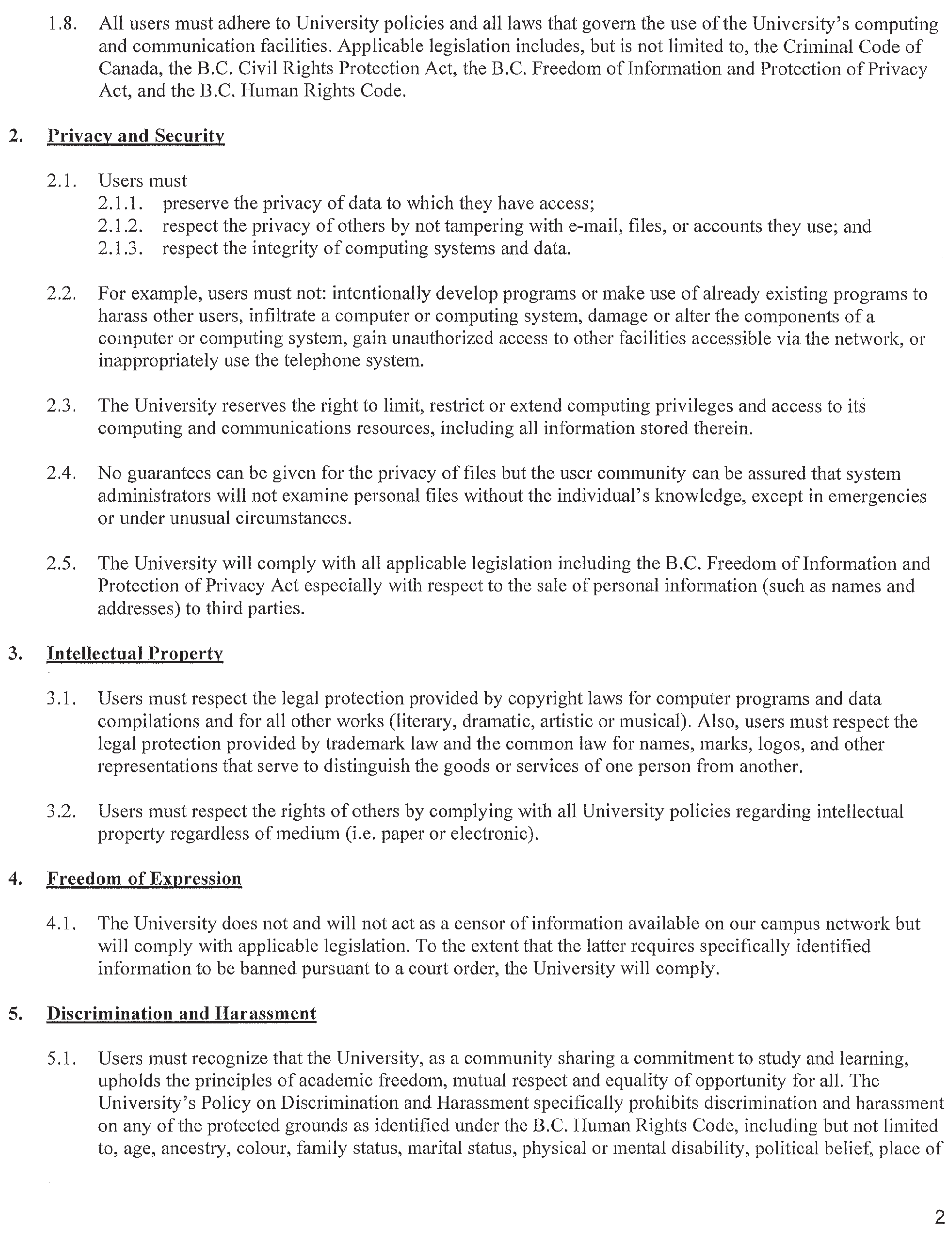
1.3. Computer IDs, accounts, and other communications facilities are to be used for authorized purposes. Incidental personal use is acceptable as long as it does not interfere with use of the facility for its intended purpose and, in the case of employees, as long as it does not interfere with his or her job performance.

1.4. Users are prohibited from accessing other users' computer IDs or accounts and communications, without specific prior authorization from the appropriate administrative head of unit.

1.5. Users are responsible for the uses to which their computing accounts are put. Users must not share the passwords to any accounts to which they have access.

1.6. Users must not misrepresent their identity as senders of messages nor the content of such messages.

1.7. Breaches of this Policy may be subject to the full range of disciplinary and other formal actions. In addition to any other sanctions that the University may levy in the event of a violation, UBC may withdraw computing privileges and network access.



1.8. All users must adhere to University policies and all laws that govern the use of the University's computing and communication facilities. Applicable legislation includes, but is not limited to, the Criminal Code of Canada, the B.C. Civil Rights Protection Act, the B.C. Freedom of Information and Protection of Privacy Act, and the B.C. Human Rights Code.

2. Privacy and Security

2.1. Users must
- 2.1.1. preserve the privacy of data to which they have access;
- 2.1.2. respect the privacy of others by not tampering with e-mail, files, or accounts they use; and
- 2.1.3. respect the integrity of computing systems and data.

2.2. For example, users must not: intentionally develop programs or make use of already existing programs to harass other users, infiltrate a computer or computing system, damage or alter the components of a computer or computing system, gain unauthorized access to other facilities accessible via the network, or inappropriately use the telephone system.

2.3. The University reserves the right to limit, restrict or extend computing privileges and access to its computing and communications resources, including all information stored therein.

2.4. No guarantees can be given for the privacy of files but the user community can be assured that system administrators will not examine personal files without the individual's knowledge, except in emergencies or under unusual circumstances.

2.5. The University will comply with all applicable legislation including the B.C. Freedom of Information and Protection of Privacy Act especially with respect to the sale of personal information (such as names and addresses) to third parties.

3. Intellectual Property

3.1. Users must respect the legal protection provided by copyright laws for computer programs and data compilations and for all other works (literary, dramatic, artistic or musical). Also, users must respect the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another.

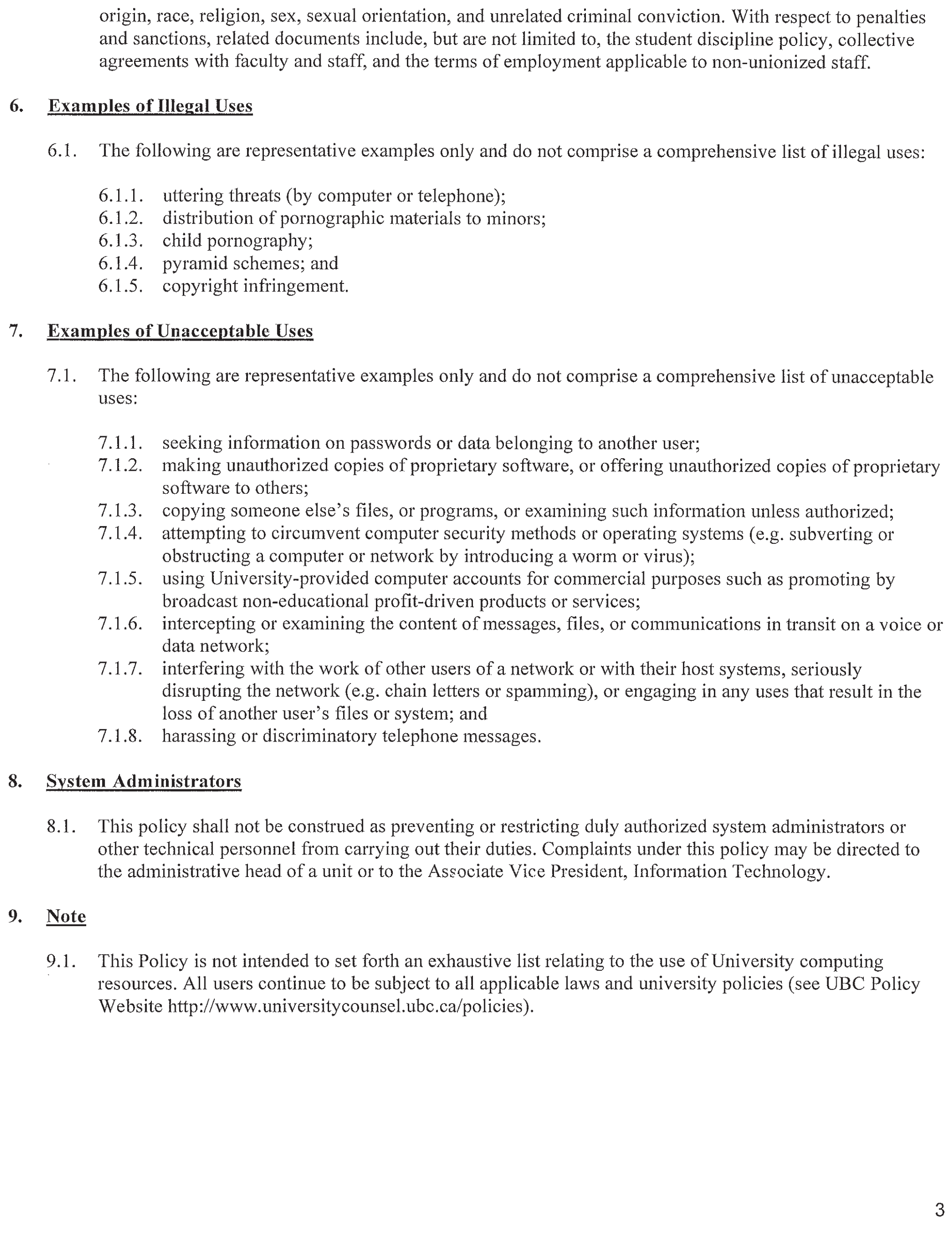
3.2. Users must respect the rights of others by complying with all University policies regarding intellectual property regardless of medium (i.e. paper or electronic).

4. Freedom of Expression

4.1. The University does not and will not act as a censor of information available on our campus network but will comply with applicable legislation. To the extent that the latter requires specifically identified information to be banned pursuant to a court order, the University will comply.

5. Discrimination and Harassment

5.1. Users must recognize that the University, as a community sharing a commitment to study and learning, upholds the principles of academic freedom, mutual respect and equality of opportunity for all. The University's Policy on Discrimination and Harassment specifically prohibits discrimination and harassment on any of the protected grounds as identified under the B.C. Human Rights Code, including but not limited to, age, ancestry, colour, family status, marital status, physical or mental disability, political belief, place of



origin, race, religion, sex, sexual orientation, and unrelated criminal conviction. With respect to penalties and sanctions, related documents include, but are not limited to, the student discipline policy, collective agreements with faculty and staff, and the terms of employment applicable to non-unionized staff.

6. Examples of Illegal Uses

6.1. The following are representative examples only and do not comprise a comprehensive list of illegal uses:

6.1.1. uttering threats (by computer or telephone);
6.1.2. distribution of pornographic materials to minors;
6.1.3. child pornography;
6.1.4. pyramid schemes; and
6.1.5. copyright infringement.

7. Examples of Unacceptable Uses

7.1. The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

7.1.1. seeking information on passwords or data belonging to another user;
7.1.2. making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
7.1.3. copying someone else's files, or programs, or examining such information unless authorized;
7.1.4. attempting to circumvent computer security methods or operating systems (e.g. subverting or obstructing a computer or network by introducing a worm or virus);
7.1.5. using University-provided computer accounts for commercial purposes such as promoting by broadcast non-educational profit-driven products or services;
7.1.6. intercepting or examining the content of messages, files, or communications in transit on a voice or data network;
7.1.7. interfering with the work of other users of a network or with their host systems, seriously disrupting the network (e.g. chain letters or spamming), or engaging in any uses that result in the loss of another user's files or system; and
7.1.8. harassing or discriminatory telephone messages.

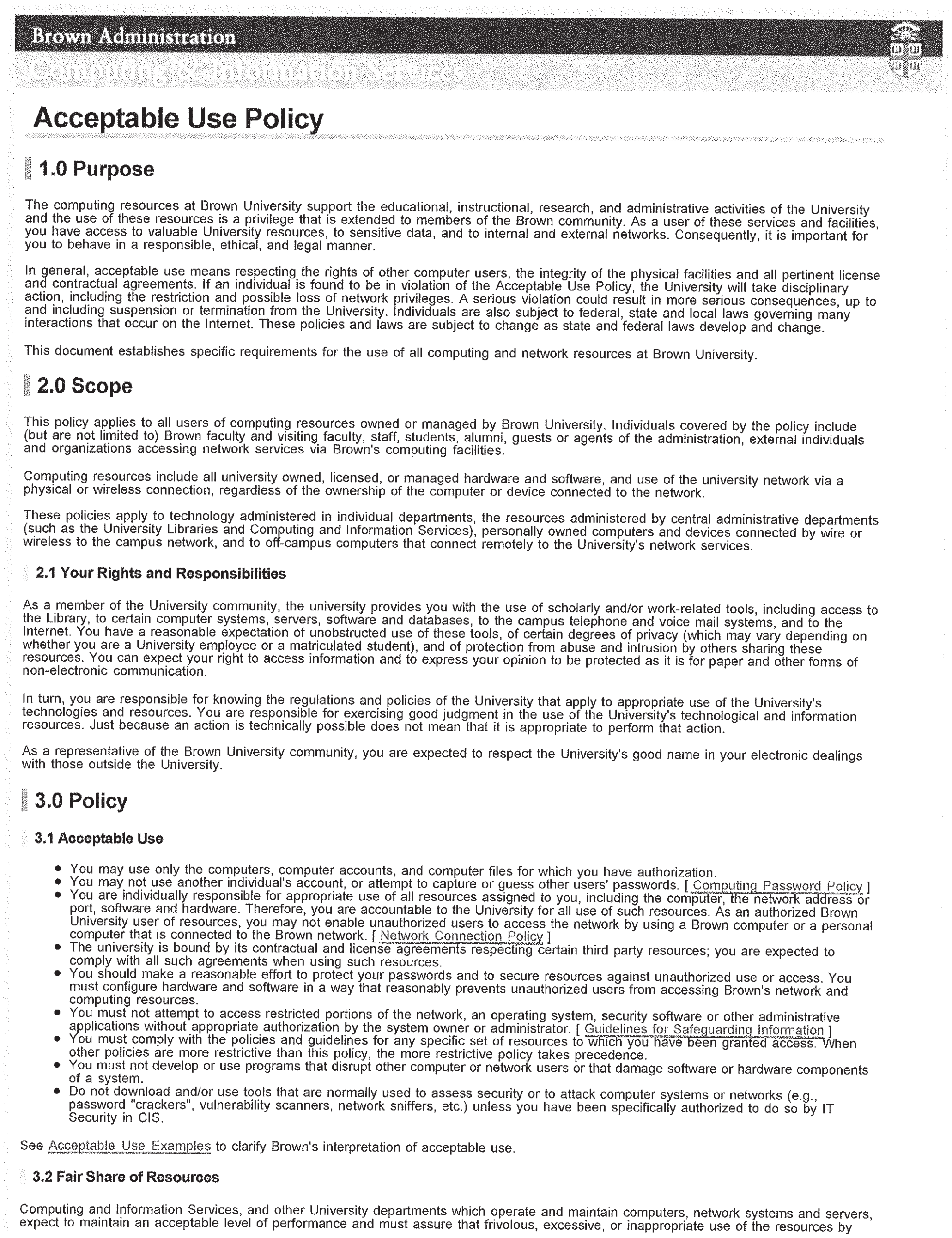
8. System Administrators

8.1. This policy shall not be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties. Complaints under this policy may be directed to the administrative head of a unit or to the Associate Vice President, Information Technology.

9. Note

9.1. This Policy is not intended to set forth an exhaustive list relating to the use of University computing resources. All users continue to be subject to all applicable laws and university policies (see UBC Policy Website http://www.universitycounsel.ubc.ca/policies).

http://brown.edu/Facilities/CIS/policy/aup.html



Brown Administration

Computing & Information Services

Acceptable Use Policy

1.0 Purpose

The computing resources at Brown University support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the Brown community. As a user of these services and facilities, you have access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at Brown University.

2.0 Scope

This policy applies to all users of computing resources owned or managed by Brown University. Individuals covered by the policy include (but are not limited to) Brown faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organizations accessing network services via Brown's computing facilities.

Computing resources include all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the University Libraries and Computing and Information Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the University's network services.

2.1 Your Rights and Responsibilities

As a member of the University community, the university provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a University employee or a matriculated student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. You are responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the Brown University community, you are expected to respect the University's good name in your electronic dealings with those outside the University.

3.0 Policy

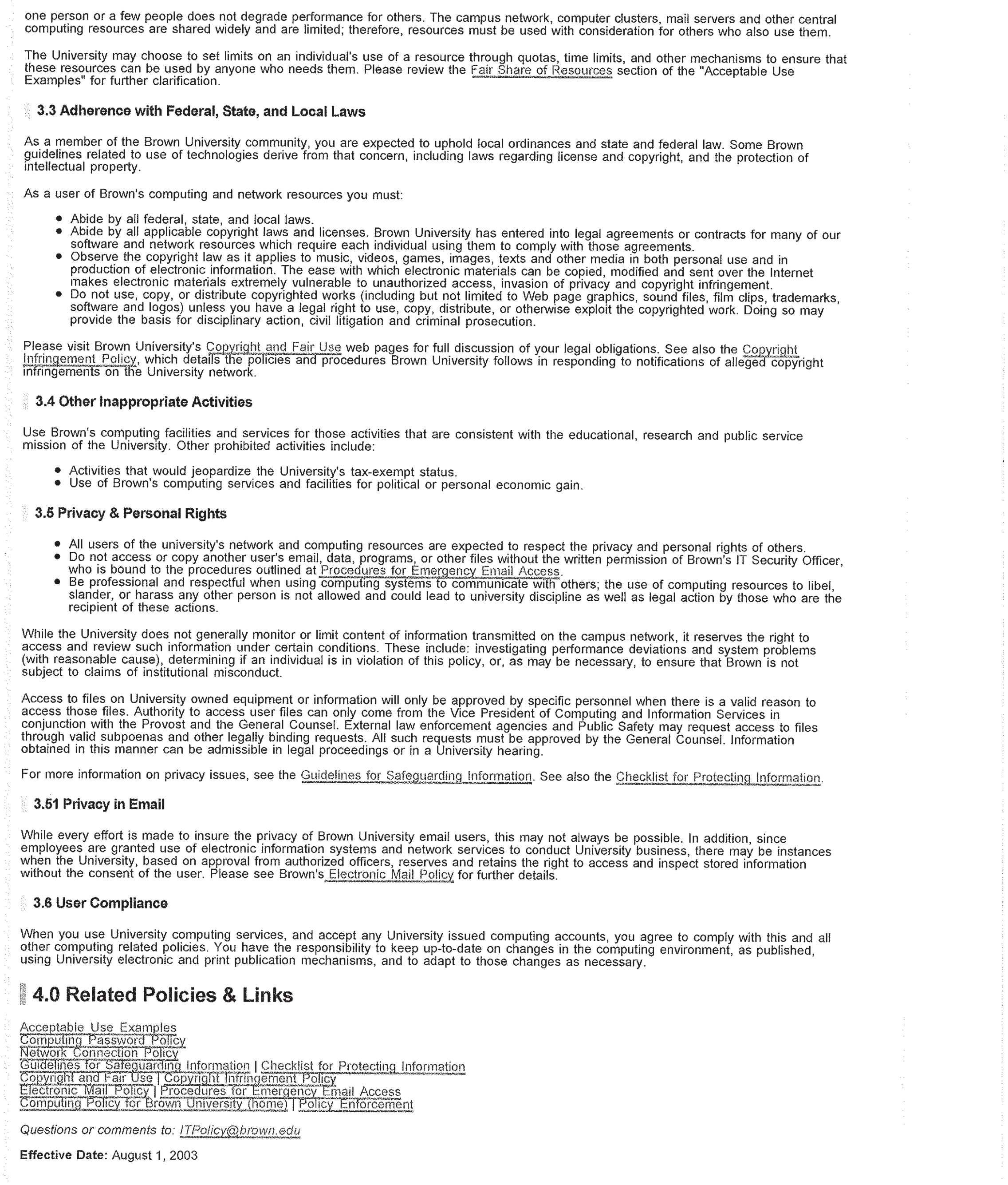
3.1 Acceptable Use

- You may use only the computers, computer accounts, and computer files for which you have authorization.
- You may not use another individual's account, or attempt to capture or guess other users' passwords. [Computing Password Policy]
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the University for all use of such resources. As an authorized Brown University user of resources, you may not enable unauthorized users to access the network by using a Brown computer or a personal computer that is connected to the Brown network. [Network Connection Policy]
- The university is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing Brown's network and computing resources.
- You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator. [Guidelines for Safeguarding Information]
- You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not develop or use programs that disrupt other computer or network users or that damage software or hardware components of a system.
- Do not download and/or use tools that are normally used to assess security or to attack computer systems or networks (e.g., password "crackers", vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by IT Security in CIS.

See Acceptable Use Examples to clarify Brown's interpretation of acceptable use.

3.2 Fair Share of Resources

Computing and Information Services, and other University departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by



one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited; therefore, resources must be used with consideration for others who also use them.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them. Please review the Fair Share of Resources section of the "Acceptable Use Examples" for further clarification.

3.3 Adherence with Federal, State, and Local Laws

As a member of the Brown University community, you are expected to uphold local ordinances and state and federal law. Some Brown guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of Brown's computing and network resources you must:

- Abide by all federal, state, and local laws.
- Abide by all applicable copyright laws and licenses. Brown University has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

Please visit Brown University's Copyright and Fair Use web pages for full discussion of your legal obligations. See also the Copyright Infringement Policy, which details the policies and procedures Brown University follows in responding to notifications of alleged copyright infringements on the University network.

3.4 Other Inappropriate Activities

Use Brown's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the University. Other prohibited activities include:

- Activities that would jeopardize the University's tax-exempt status.
- Use of Brown's computing services and facilities for political or personal economic gain.

3.5 Privacy & Personal Rights

- All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without the written permission of Brown's IT Security Officer, who is bound to the procedures outlined at Procedures for Emergency Email Access.
- Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.

While the University does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that Brown is not subject to claims of institutional misconduct.

Access to files on University owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Vice President of Computing and Information Services in conjunction with the Provost and the General Counsel. External law enforcement agencies and Public Safety may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the General Counsel. Information obtained in this manner can be admissible in legal proceedings or in a University hearing.

For more information on privacy issues, see the Guidelines for Safeguarding Information. See also the Checklist for Protecting Information.

3.51 Privacy in Email

While every effort is made to insure the privacy of Brown University email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user. Please see Brown's Electronic Mail Policy for further details.

3.6 User Compliance

When you use University computing services, and accept any University issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using University electronic and print publication mechanisms, and to adapt to those changes as necessary.

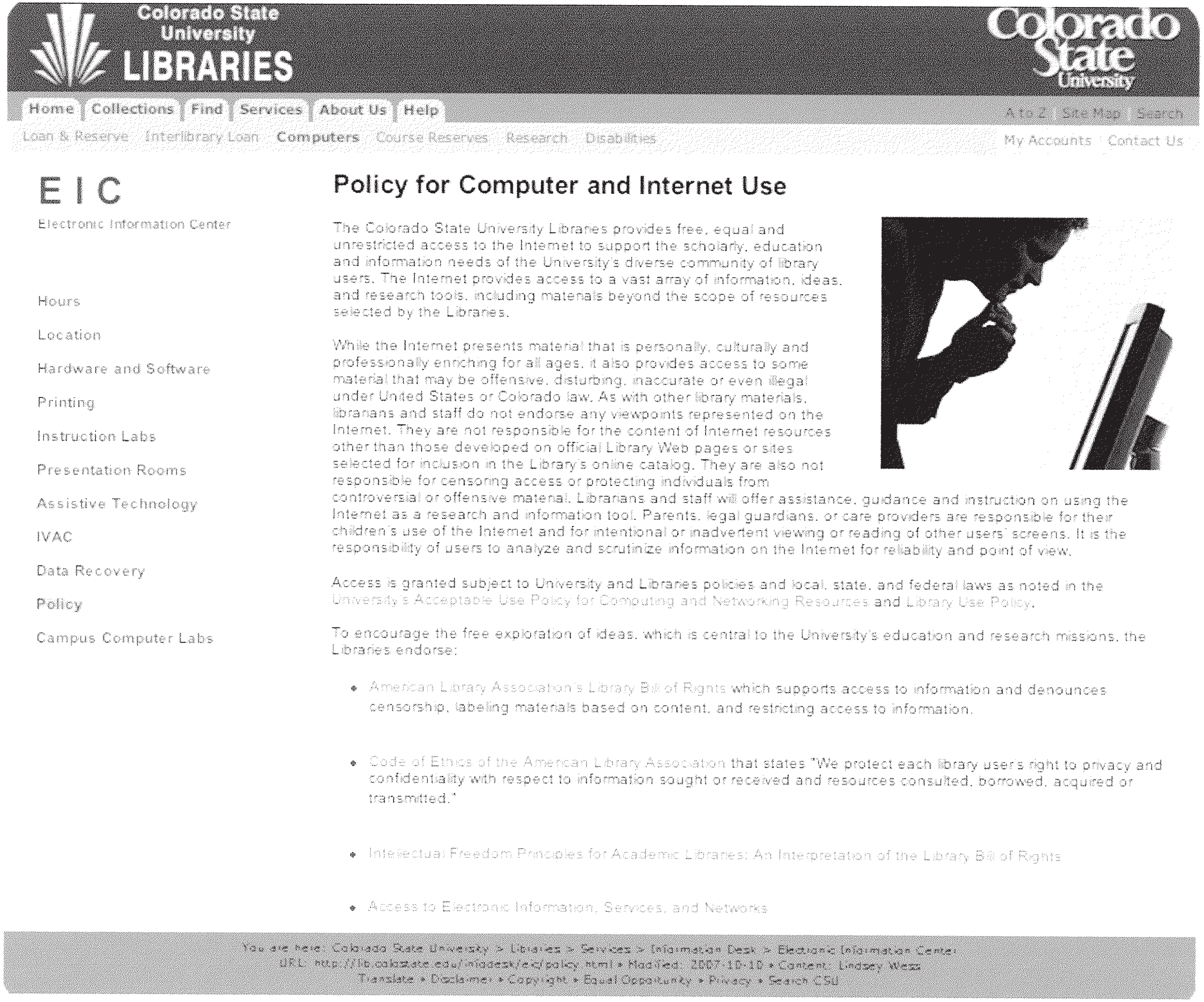
4.0 Related Policies & Links

Acceptable Use Examples
Computing Password Policy
Network Connection Policy
Guidelines for Safeguarding Information | Checklist for Protecting Information
Copyright and Fair Use | Copyright Infringement Policy
Electronic Mail Policy | Procedures for Emergency Email Access
Computing Policy for Brown University (home) | Policy Enforcement

Questions or comments to: ITPolicy@brown.edu

Effective Date: August 1, 2003

http://lib.colostate.edu/infodesk/eic/policy.html



Colorado State University LIBRARIES
Colorado State University
Home | Collections | Find | Services | About Us | Help
A to Z | Site Map | Search
Loan & Reserve | Interlibrary Loan | Computers | Course Reserves | Research | Disabilities
My Accounts | Contact Us
E I C
Electronic Information Center
Hours
Location
Hardware and Software
Printing
Instruction Labs
Presentation Rooms
Assistive Technology
IVAC
Data Recovery
Policy
Campus Computer Labs

Policy for Computer and Internet Use

The Colorado State University Libraries provides free, equal and unrestricted access to the Internet to support the scholarly, education and information needs of the University's diverse community of library users. The Internet provides access to a vast array of information, ideas, and research tools, including materials beyond the scope of resources selected by the Libraries.

While the Internet presents material that is personally, culturally and professionally enriching for all ages, it also provides access to some material that may be offensive, disturbing, inaccurate or even illegal under United States or Colorado law. As with other library materials, librarians and staff do not endorse any viewpoints represented on the Internet. They are not responsible for the content of Internet resources other than those developed on official Library Web pages or sites selected for inclusion in the Library's online catalog. They are also not responsible for censoring access or protecting individuals from controversial or offensive material. Librarians and staff will offer assistance, guidance and instruction on using the Internet as a research and information tool. Parents, legal guardians, or care providers are responsible for their children's use of the Internet and for intentional or inadvertent viewing or reading of other users' screens. It is the responsibility of users to analyze and scrutinize information on the Internet for reliability and point of view.

Access is granted subject to University and Libraries policies and local, state, and federal laws as noted in the University's Acceptable Use Policy for Computing and Networking Resources and Library Use Policy.

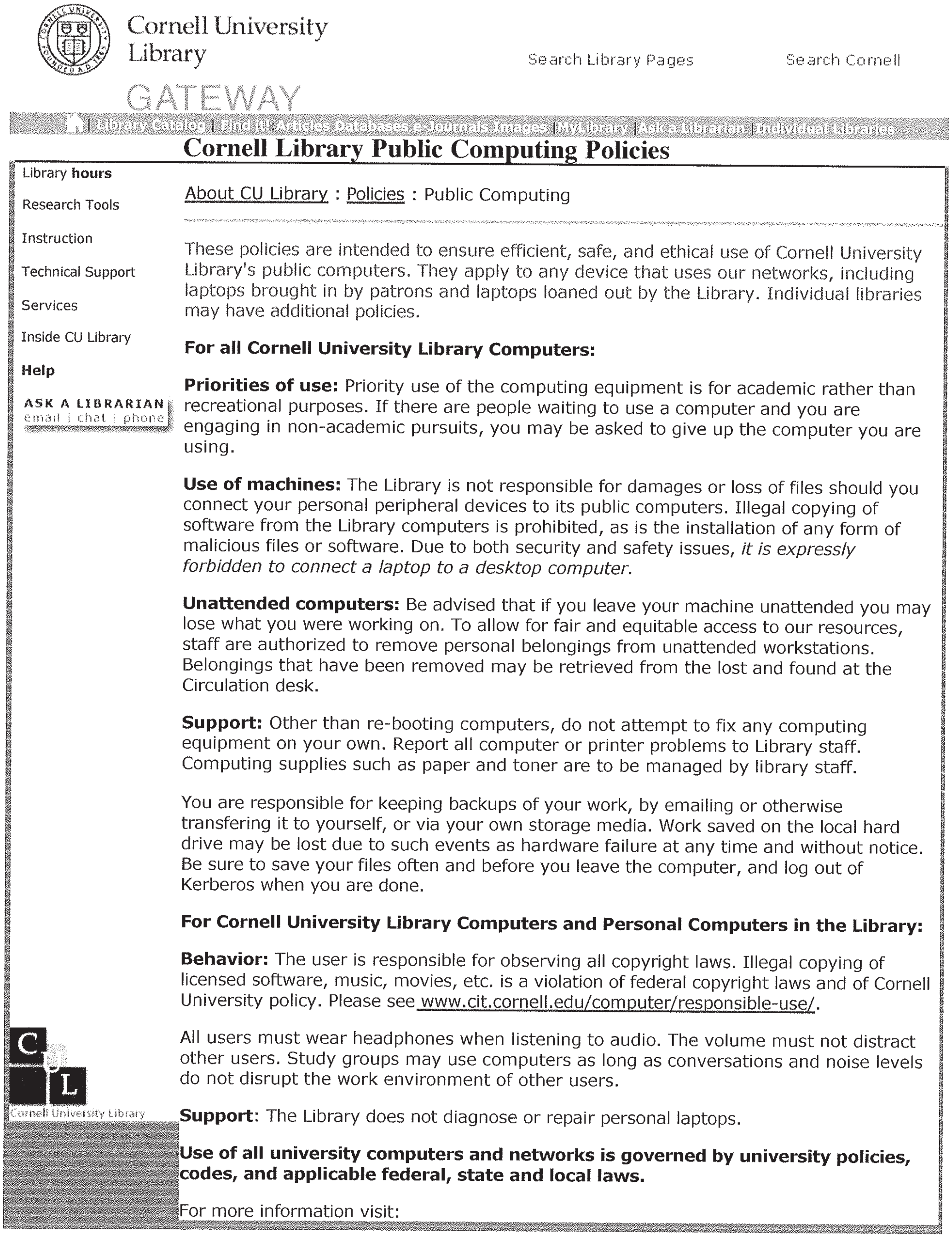
To encourage the free exploration of ideas, which is central to the University's education and research missions, the Libraries endorse:

- American Library Association's Library Bill of Rights which supports access to information and denounces censorship, labeling materials based on content, and restricting access to information.
- Code of Ethics of the American Library Association that states "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."
- Intellectual Freedom Principles for Academic Libraries: An Interpretation of the Library Bill of Rights
- Access to Electronic Information, Services, and Networks

You are here: Colorado State University > Libraries > Services > Information Desk > Electronic Information Center
URL: http://lib.colostate.edu/infodesk/eic/policy.html • Modified: 2007-10-10 • Content: Lindsey Wess
Translate • Disclaimer • Copyright • Equal Opportunity • Privacy • Search CSU

CORNELL UNIVERSITY

http://www.library.cornell.edu/about/policyPublicComputing.html



Cornell Library Public Computing Policies

About CU Library : Policies : Public Computing

These policies are intended to ensure efficient, safe, and ethical use of Cornell University Library's public computers. They apply to any device that uses our networks, including laptops brought in by patrons and laptops loaned out by the Library. Individual libraries may have additional policies.

For all Cornell University Library Computers:

Priorities of use: Priority use of the computing equipment is for academic rather than recreational purposes. If there are people waiting to use a computer and you are engaging in non-academic pursuits, you may be asked to give up the computer you are using.

Use of machines: The Library is not responsible for damages or loss of files should you connect your personal peripheral devices to its public computers. Illegal copying of software from the Library computers is prohibited, as is the installation of any form of malicious files or software. Due to both security and safety issues, *it is expressly forbidden to connect a laptop to a desktop computer.*

Unattended computers: Be advised that if you leave your machine unattended you may lose what you were working on. To allow for fair and equitable access to our resources, staff are authorized to remove personal belongings from unattended workstations. Belongings that have been removed may be retrieved from the lost and found at the Circulation desk.

Support: Other than re-booting computers, do not attempt to fix any computing equipment on your own. Report all computer or printer problems to Library staff. Computing supplies such as paper and toner are to be managed by library staff.

You are responsible for keeping backups of your work, by emailing or otherwise transfering it to yourself, or via your own storage media. Work saved on the local hard drive may be lost due to such events as hardware failure at any time and without notice. Be sure to save your files often and before you leave the computer, and log out of Kerberos when you are done.

For Cornell University Library Computers and Personal Computers in the Library:

Behavior: The user is responsible for observing all copyright laws. Illegal copying of licensed software, music, movies, etc. is a violation of federal copyright laws and of Cornell University policy. Please see www.cit.cornell.edu/computer/responsible-use/.

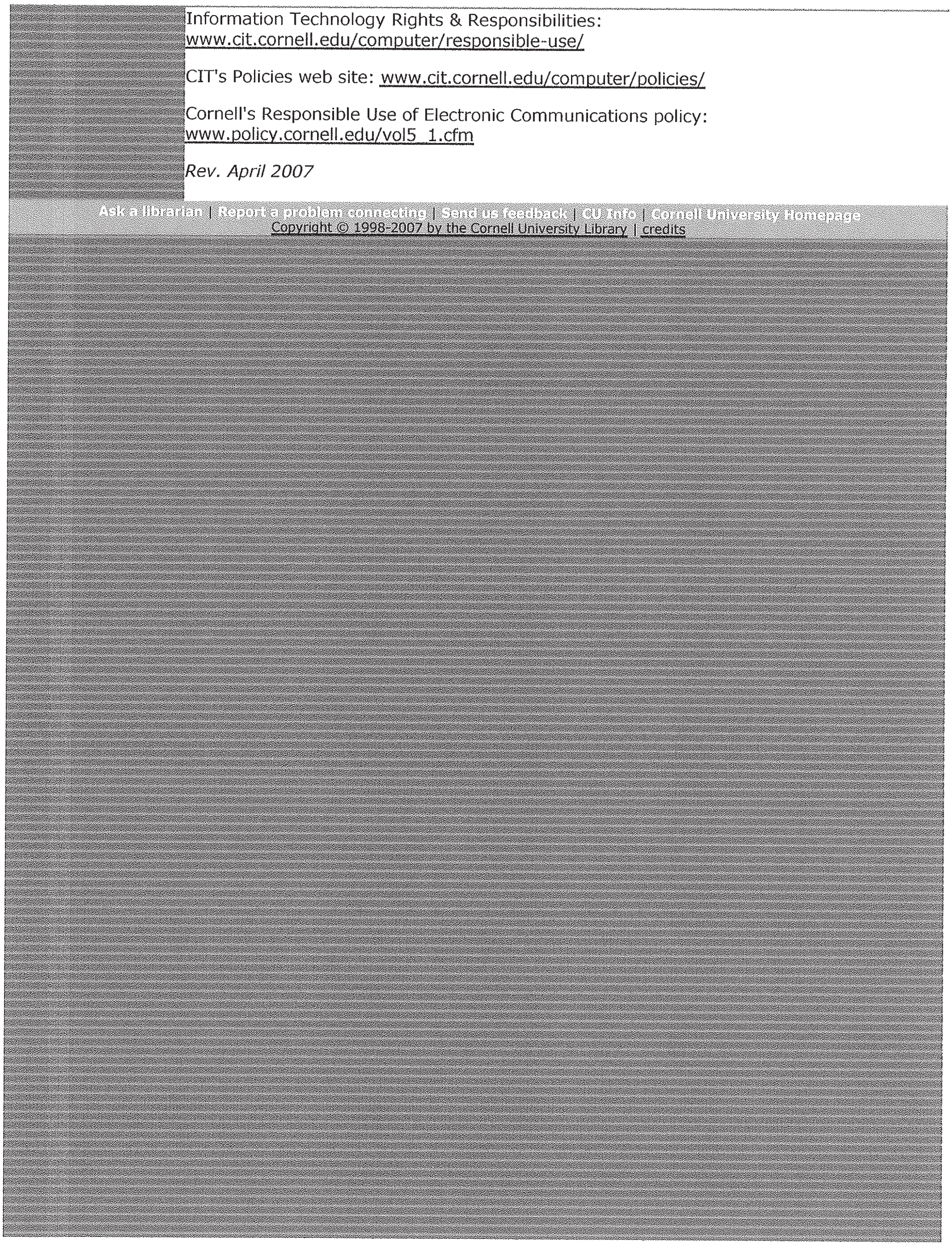
All users must wear headphones when listening to audio. The volume must not distract other users. Study groups may use computers as long as conversations and noise levels do not disrupt the work environment of other users.

Support: The Library does not diagnose or repair personal laptops.

Use of all university computers and networks is governed by university policies, codes, and applicable federal, state and local laws.

For more information visit:

http://www.library.cornell.edu/about/policyPublicComputing.html



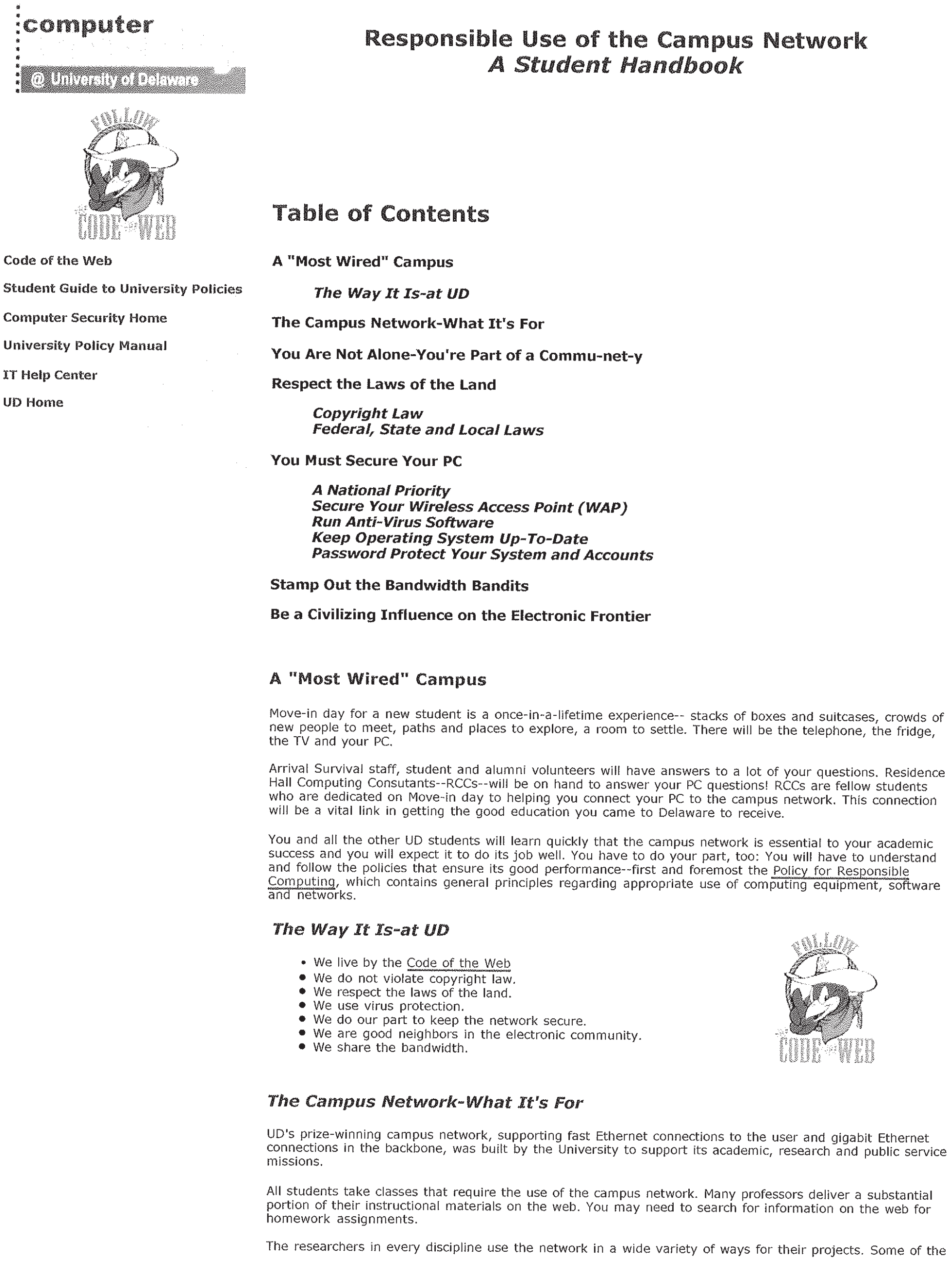
Information Technology Rights & Responsibilities:
www.cit.cornell.edu/computer/responsible-use/

CIT's Policies web site: www.cit.cornell.edu/computer/policies/

Cornell's Responsible Use of Electronic Communications policy:
www.policy.cornell.edu/vol5_1.cfm

Rev. April 2007

Ask a librarian | Report a problem connecting | Send us feedback | CU Info | Cornell University Homepage http://www.udel.edu/ecce/student-toc.html



Code of the Web

Student Guide to University Policies

Computer Security Home

University Policy Manual

IT Help Center

UD Home

Responsible Use of the Campus Network
A Student Handbook

Table of Contents

A "Most Wired" Campus

Move-in day for a new student is a once-in-a-lifetime experience-- stacks of boxes and suitcases, crowds of new people to meet, paths and places to explore, a room to settle. There will be the telephone, the fridge, the TV and your PC.

Arrival Survival staff, student and alumni volunteers will have answers to a lot of your questions. Residence Hall Computing Consutants--RCCs--will be on hand to answer your PC questions! RCCs are fellow students who are dedicated on Move-in day to helping you connect your PC to the campus network. This connection will be a vital link in getting the good education you came to Delaware to receive.

You and all the other UD students will learn quickly that the campus network is essential to your academic success and you will expect it to do its job well. You have to do your part, too: You will have to understand and follow the policies that ensure its good performance--first and foremost the Policy for Responsible Computing, which contains general principles regarding appropriate use of computing equipment, software and networks.

The Way It Is-at UD

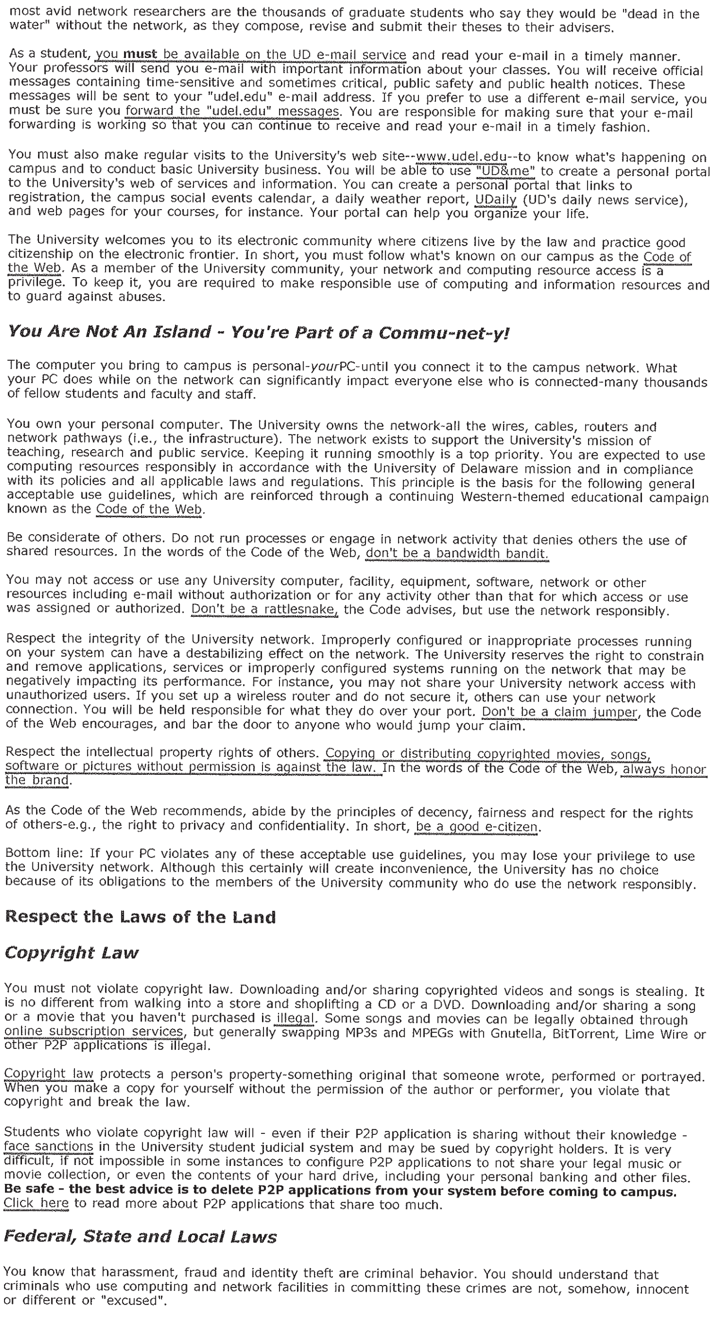
- We live by the Code of the Web
- We do not violate copyright law.
- We respect the laws of the land.
- We use virus protection.
- We do our part to keep the network secure.
- We are good neighbors in the electronic community.
- We share the bandwidth.

The Campus Network-What It's For

UD's prize-winning campus network, supporting fast Ethernet connections to the user and gigabit Ethernet connections in the backbone, was built by the University to support its academic, research and public service missions.

All students take classes that require the use of the campus network. Many professors deliver a substantial portion of their instructional materials on the web. You may need to search for information on the web for homework assignments.

The researchers in every discipline use the network in a wide variety of ways for their projects. Some of the



most avid network researchers are the thousands of graduate students who say they would be "dead in the water" without the network, as they compose, revise and submit their theses to their advisers.

As a student, you **must** be available on the UD e-mail service and read your e-mail in a timely manner. Your professors will send you e-mail with important information about your classes. You will receive official messages containing time-sensitive and sometimes critical, public safety and public health notices. These messages will be sent to your "udel.edu" e-mail address. If you prefer to use a different e-mail service, you must be sure you forward the "udel.edu" messages. You are responsible for making sure that your e-mail forwarding is working so that you can continue to receive and read your e-mail in a timely fashion.

You must also make regular visits to the University's web site--www.udel.edu--to know what's happening on campus and to conduct basic University business. You will be able to use "UD&me" to create a personal portal to the University's web of services and information. You can create a personal portal that links to registration, the campus social events calendar, a daily weather report, UDaily (UD's daily news service), and web pages for your courses, for instance. Your portal can help you organize your life.

The University welcomes you to its electronic community where citizens live by the law and practice good citizenship on the electronic frontier. In short, you must follow what's known on our campus as the Code of the Web. As a member of the University community, your network and computing resource access is a privilege. To keep it, you are required to make responsible use of computing and information resources and to guard against abuses.

You Are Not An Island - You're Part of a Commu-net-y!

The computer you bring to campus is personal-*your*PC-until you connect it to the campus network. What your PC does while on the network can significantly impact everyone else who is connected-many thousands of fellow students and faculty and staff.

You own your personal computer. The University owns the network-all the wires, cables, routers and network pathways (i.e., the infrastructure). The network exists to support the University's mission of teaching, research and public service. Keeping it running smoothly is a top priority. You are expected to use computing resources responsibly in accordance with the University of Delaware mission and in compliance with its policies and all applicable laws and regulations. This principle is the basis for the following general acceptable use guidelines, which are reinforced through a continuing Western-themed educational campaign known as the Code of the Web.

Be considerate of others. Do not run processes or engage in network activity that denies others the use of shared resources. In the words of the Code of the Web, don't be a bandwidth bandit.

You may not access or use any University computer, facility, equipment, software, network or other resources including e-mail without authorization or for any activity other than that for which access or use was assigned or authorized. Don't be a rattlesnake, the Code advises, but use the network responsibly.

Respect the integrity of the University network. Improperly configured or inappropriate processes running on your system can have a destabilizing effect on the network. The University reserves the right to constrain and remove applications, services or improperly configured systems running on the network that may be negatively impacting its performance. For instance, you may not share your University network access with unauthorized users. If you set up a wireless router and do not secure it, others can use your network connection. You will be held responsible for what they do over your port. Don't be a claim jumper, the Code of the Web encourages, and bar the door to anyone who would jump your claim.

Respect the intellectual property rights of others. Copying or distributing copyrighted movies, songs, software or pictures without permission is against the law. In the words of the Code of the Web, always honor the brand.

As the Code of the Web recommends, abide by the principles of decency, fairness and respect for the rights of others-e.g., the right to privacy and confidentiality. In short, be a good e-citizen.

Bottom line: If your PC violates any of these acceptable use guidelines, you may lose your privilege to use the University network. Although this certainly will create inconvenience, the University has no choice because of its obligations to the members of the University community who do use the network responsibly.

Respect the Laws of the Land

Copyright Law

You must not violate copyright law. Downloading and/or sharing copyrighted videos and songs is stealing. It is no different from walking into a store and shoplifting a CD or a DVD. Downloading and/or sharing a song or a movie that you haven't purchased is illegal. Some songs and movies can be legally obtained through online subscription services, but generally swapping MP3s and MPEGs with Gnutella, BitTorrent, Lime Wire or other P2P applications is illegal.

Copyright law protects a person's property-something original that someone wrote, performed or portrayed. When you make a copy for yourself without the permission of the author or performer, you violate that copyright and break the law.

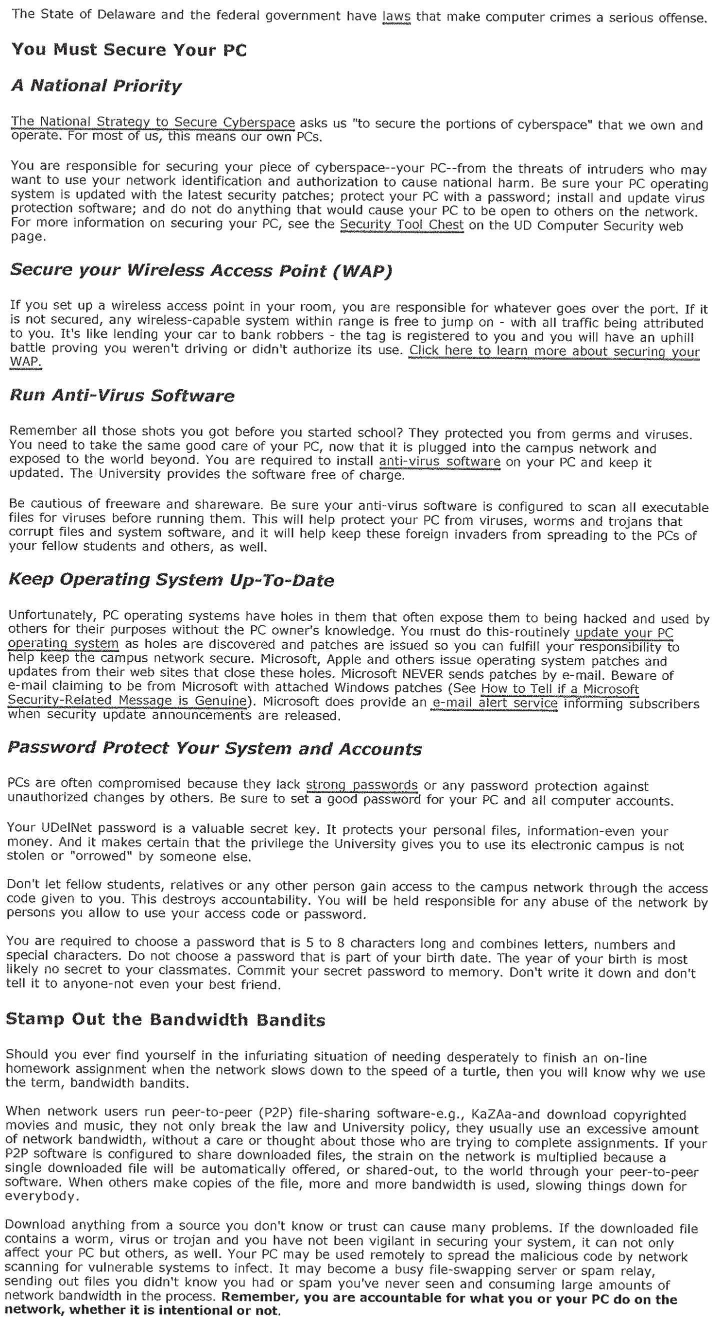
Students who violate copyright law will - even if their P2P application is sharing without their knowledge - face sanctions in the University student judicial system and may be sued by copyright holders. It is very difficult, if not impossible in some instances to configure P2P applications to not share your legal music or movie collection, or even the contents of your hard drive, including your personal banking and other files. **Be safe - the best advice is to delete P2P applications from your system before coming to campus.** Click here to read more about P2P applications that share too much.

Federal, State and Local Laws

You know that harassment, fraud and identity theft are criminal behavior. You should understand that criminals who use computing and network facilities in committing these crimes are not, somehow, innocent or different or "excused".

UNIVERSITY OF DELAWARE

http://www.udel.edu/ecce/student-toc.html



The State of Delaware and the federal government have laws that make computer crimes a serious offense.

You Must Secure Your PC

A National Priority

The National Strategy to Secure Cyberspace asks us "to secure the portions of cyberspace" that we own and operate. For most of us, this means our own PCs.

You are responsible for securing your piece of cyberspace--your PC--from the threats of intruders who may want to use your network identification and authorization to cause national harm. Be sure your PC operating system is updated with the latest security patches; protect your PC with a password; install and update virus protection software; and do not do anything that would cause your PC to be open to others on the network. For more information on securing your PC, see the Security Tool Chest on the UD Computer Security web page.

Secure your Wireless Access Point (WAP)

If you set up a wireless access point in your room, you are responsible for whatever goes over the port. If it is not secured, any wireless-capable system within range is free to jump on - with all traffic being attributed to you. It's like lending your car to bank robbers - the tag is registered to you and you will have an uphill battle proving you weren't driving or didn't authorize its use. Click here to learn more about securing your WAP.

Run Anti-Virus Software

Remember all those shots you got before you started school? They protected you from germs and viruses. You need to take the same good care of your PC, now that it is plugged into the campus network and exposed to the world beyond. You are required to install anti-virus software on your PC and keep it updated. The University provides the software free of charge.

Be cautious of freeware and shareware. Be sure your anti-virus software is configured to scan all executable files for viruses before running them. This will help protect your PC from viruses, worms and trojans that corrupt files and system software, and it will help keep these foreign invaders from spreading to the PCs of your fellow students and others, as well.

Keep Operating System Up-To-Date

Unfortunately, PC operating systems have holes in them that often expose them to being hacked and used by others for their purposes without the PC owner's knowledge. You must do this-routinely update your PC operating system as holes are discovered and patches are issued so you can fulfill your responsibility to help keep the campus network secure. Microsoft, Apple and others issue operating system patches and updates from their web sites that close these holes. Microsoft NEVER sends patches by e-mail. Beware of e-mail claiming to be from Microsoft with attached Windows patches (See How to Tell if a Microsoft Security-Related Message is Genuine). Microsoft does provide an e-mail alert service informing subscribers when security update announcements are released.

Password Protect Your System and Accounts

PCs are often compromised because they lack strong passwords or any password protection against unauthorized changes by others. Be sure to set a good password for your PC and all computer accounts.

Your UDelNet password is a valuable secret key. It protects your personal files, information-even your money. And it makes certain that the privilege the University gives you to use its electronic campus is not stolen or "orrowed" by someone else.

Don't let fellow students, relatives or any other person gain access to the campus network through the access code given to you. This destroys accountability. You will be held responsible for any abuse of the network by persons you allow to use your access code or password.

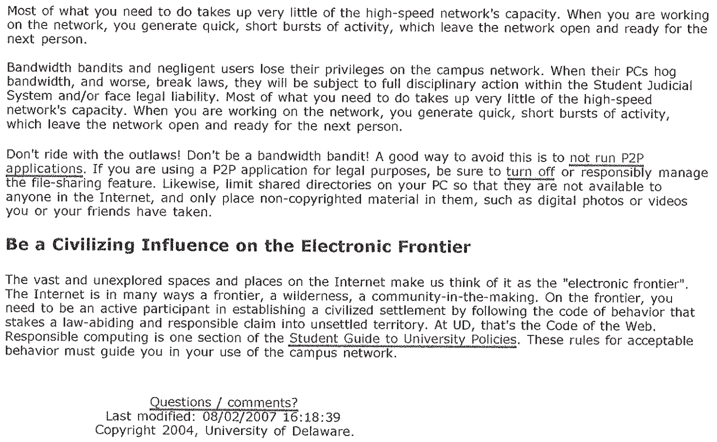
You are required to choose a password that is 5 to 8 characters long and combines letters, numbers and special characters. Do not choose a password that is part of your birth date. The year of your birth is most likely no secret to your classmates. Commit your secret password to memory. Don't write it down and don't tell it to anyone-not even your best friend.

Stamp Out the Bandwidth Bandits

Should you ever find yourself in the infuriating situation of needing desperately to finish an on-line homework assignment when the network slows down to the speed of a turtle, then you will know why we use the term, bandwidth bandits.

When network users run peer-to-peer (P2P) file-sharing software-e.g., KaZAa-and download copyrighted movies and music, they not only break the law and University policy, they usually use an excessive amount of network bandwidth, without a care or thought about those who are trying to complete assignments. If your P2P software is configured to share downloaded files, the strain on the network is multiplied because a single downloaded file will be automatically offered, or shared-out, to the world through your peer-to-peer software. When others make copies of the file, more and more bandwidth is used, slowing things down for everybody.

Download anything from a source you don't know or trust can cause many problems. If the downloaded file contains a worm, virus or trojan and you have not been vigilant in securing your system, it can not only affect your PC but others, as well. Your PC may be used remotely to spread the malicious code by network scanning for vulnerable systems to infect. It may become a busy file-swapping server or spam relay, sending out files you didn't know you had or spam you've never seen and consuming large amounts of network bandwidth in the process. **Remember, you are accountable for what you or your PC do on the network, whether it is intentional or not.**



Most of what you need to do takes up very little of the high-speed network's capacity. When you are working on the network, you generate quick, short bursts of activity, which leave the network open and ready for the next person.

Bandwidth bandits and negligent users lose their privileges on the campus network. When their PCs hog bandwidth, and worse, break laws, they will be subject to full disciplinary action within the Student Judicial System and/or face legal liability. Most of what you need to do takes up very little of the high-speed network's capacity. When you are working on the network, you generate quick, short bursts of activity, which leave the network open and ready for the next person.

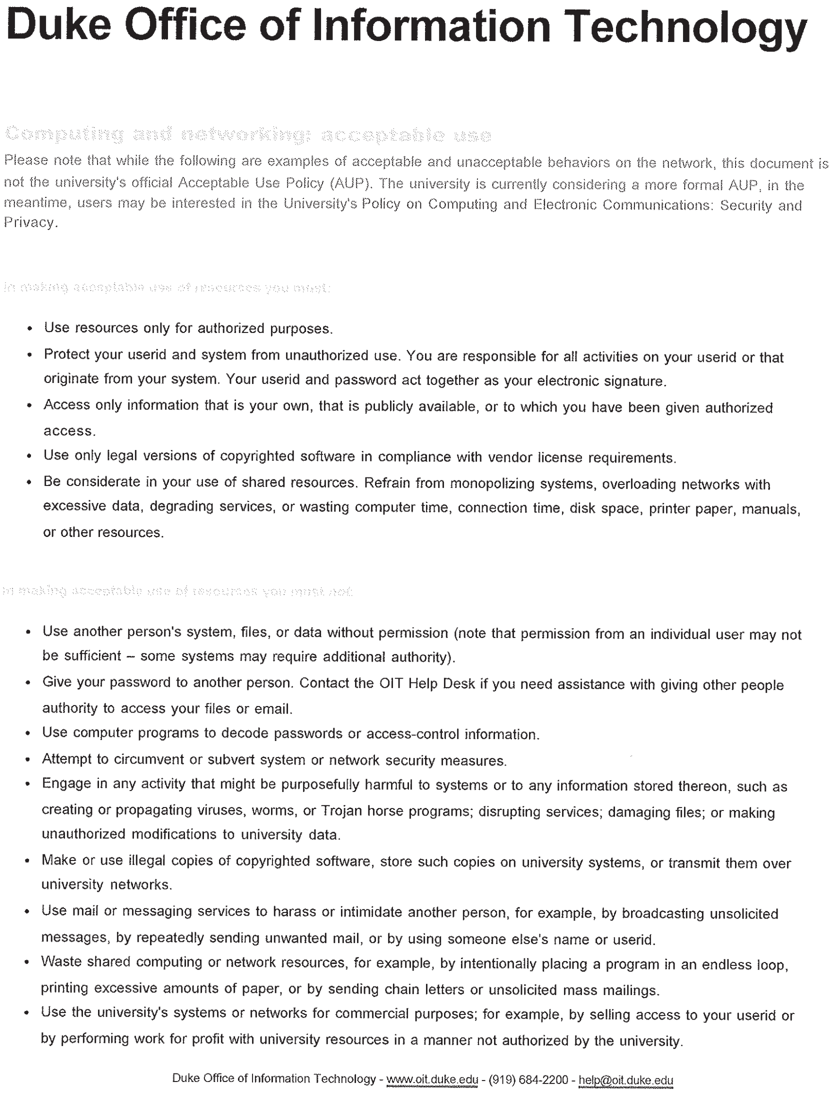
Don't ride with the outlaws! Don't be a bandwidth bandit! A good way to avoid this is to not run P2P applications. If you are using a P2P application for legal purposes, be sure to turn off or responsibly manage the file-sharing feature. Likewise, limit shared directories on your PC so that they are not available to anyone in the Internet, and only place non-copyrighted material in them, such as digital photos or videos you or your friends have taken.

Be a Civilizing Influence on the Electronic Frontier

The vast and unexplored spaces and places on the Internet make us think of it as the "electronic frontier". The Internet is in many ways a frontier, a wilderness, a community-in-the-making. On the frontier, you need to be an active participant in establishing a civilized settlement by following the code of behavior that stakes a law-abiding and responsible claim into unsettled territory. At UD, that's the Code of the Web. Responsible computing is one section of the Student Guide to University Policies. These rules for acceptable behavior must guide you in your use of the campus network.

Questions / comments?
Last modified: 08/02/2007 16:18:39

http://www.oit.duke.edu/netid-security/security/policy/acceptableuse.html



Duke Office of Information Technology

Computing and networking: acceptable use

Please note that while the following are examples of acceptable and unacceptable behaviors on the network, this document is not the university's official Acceptable Use Policy (AUP). The university is currently considering a more formal AUP, in the meantime, users may be interested in the University's Policy on Computing and Electronic Communications: Security and Privacy.

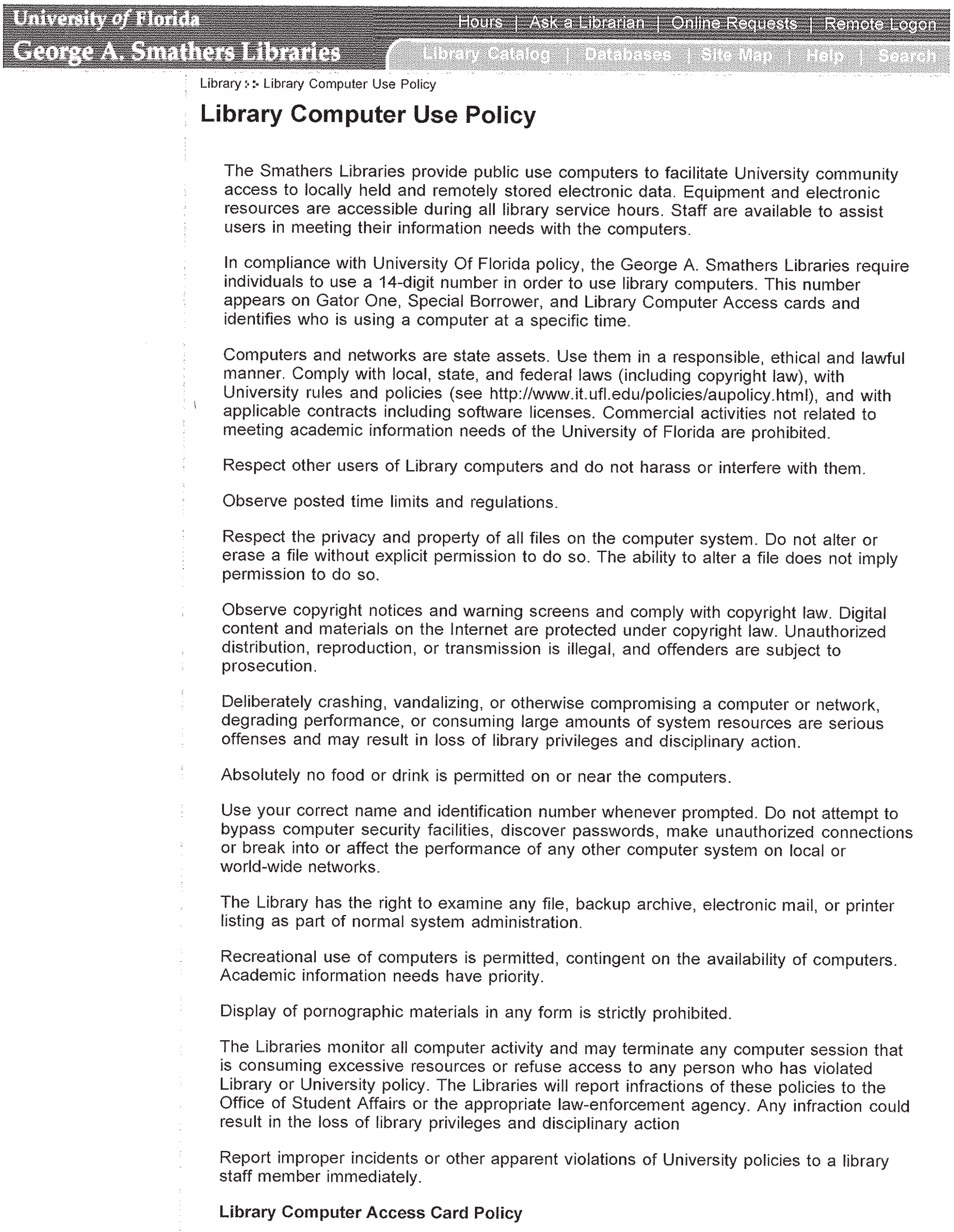
In making acceptable use of resources you must:

- Use resources only for authorized purposes.
- Protect your userid and system from unauthorized use. You are responsible for all activities on your userid or that originate from your system. Your userid and password act together as your electronic signature.
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.

In making acceptable use of resources you must not:

- Use another person's system, files, or data without permission (note that permission from an individual user may not be sufficient – some systems may require additional authority).
- Give your password to another person. Contact the OIT Help Desk if you need assistance with giving other people authority to access your files or email.
- Use computer programs to decode passwords or access-control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, worms, or Trojan horse programs; disrupting services; damaging files; or making unauthorized modifications to university data.
- Make or use illegal copies of copyrighted software, store such copies on university systems, or transmit them over university networks.
- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or userid.
- Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the university's systems or networks for commercial purposes; for example, by selling access to your userid or by performing work for profit with university resources in a manner not authorized by the university.

Duke Office of Information Technology - www.oit.duke.edu - (919) 684-2200 - help@oit.duke.edu http://www.uflib.ufl.edu/computeruse.html


University of Florida
George A. Smathers Libraries
Hours | Ask a Librarian | Online Requests | Remote Logon
Library Catalog | Databases | Site Map | Help | Search
Library :: Library Computer Use Policy

Library Computer Use Policy

The Smathers Libraries provide public use computers to facilitate University community access to locally held and remotely stored electronic data. Equipment and electronic resources are accessible during all library service hours. Staff are available to assist users in meeting their information needs with the computers.

In compliance with University Of Florida policy, the George A. Smathers Libraries require individuals to use a 14-digit number in order to use library computers. This number appears on Gator One, Special Borrower, and Library Computer Access cards and identifies who is using a computer at a specific time.

Computers and networks are state assets. Use them in a responsible, ethical and lawful manner. Comply with local, state, and federal laws (including copyright law), with University rules and policies (see http://www.it.ufl.edu/policies/aupolicy.html), and with applicable contracts including software licenses. Commercial activities not related to meeting academic information needs of the University of Florida are prohibited.

Respect other users of Library computers and do not harass or interfere with them.

Observe posted time limits and regulations.

Respect the privacy and property of all files on the computer system. Do not alter or erase a file without explicit permission to do so. The ability to alter a file does not imply permission to do so.

Observe copyright notices and warning screens and comply with copyright law. Digital content and materials on the Internet are protected under copyright law. Unauthorized distribution, reproduction, or transmission is illegal, and offenders are subject to prosecution.

Deliberately crashing, vandalizing, or otherwise compromising a computer or network, degrading performance, or consuming large amounts of system resources are serious offenses and may result in loss of library privileges and disciplinary action.

Absolutely no food or drink is permitted on or near the computers.

Use your correct name and identification number whenever prompted. Do not attempt to bypass computer security facilities, discover passwords, make unauthorized connections or break into or affect the performance of any other computer system on local or world-wide networks.

The Library has the right to examine any file, backup archive, electronic mail, or printer listing as part of normal system administration.

Recreational use of computers is permitted, contingent on the availability of computers. Academic information needs have priority.

Display of pornographic materials in any form is strictly prohibited.

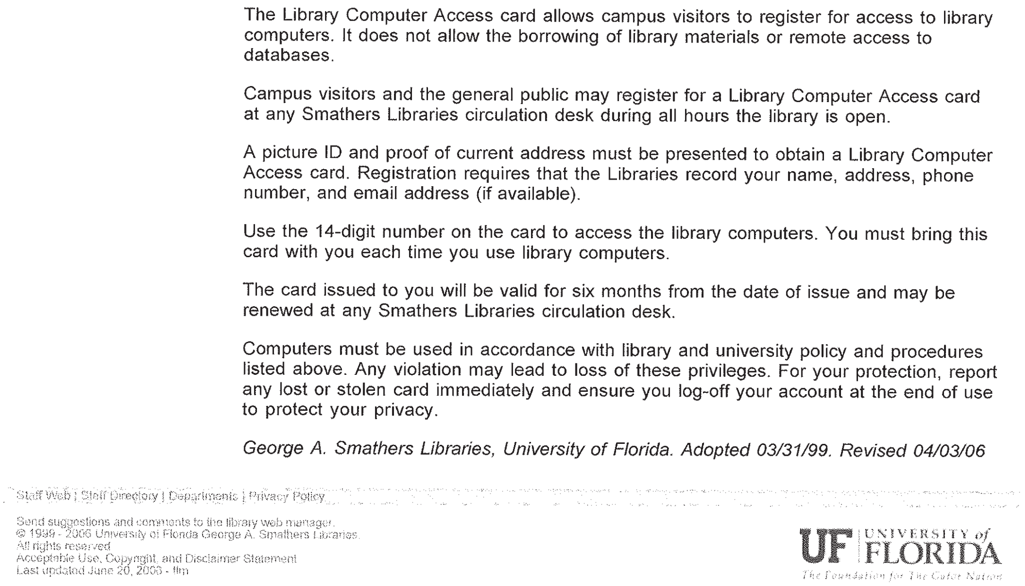
The Libraries monitor all computer activity and may terminate any computer session that is consuming excessive resources or refuse access to any person who has violated Library or University policy. The Libraries will report infractions of these policies to the Office of Student Affairs or the appropriate law-enforcement agency. Any infraction could result in the loss of library privileges and disciplinary action

Report improper incidents or other apparent violations of University policies to a library staff member immediately.

Library Computer Access Card Policy

UNIVERSITY OF FLORIDA

http://www.uflib.ufl.edu/computeruse.html



The Library Computer Access card allows campus visitors to register for access to library computers. It does not allow the borrowing of library materials or remote access to databases.

Campus visitors and the general public may register for a Library Computer Access card at any Smathers Libraries circulation desk during all hours the library is open.

A picture ID and proof of current address must be presented to obtain a Library Computer Access card. Registration requires that the Libraries record your name, address, phone number, and email address (if available).

Use the 14-digit number on the card to access the library computers. You must bring this card with you each time you use library computers.

The card issued to you will be valid for six months from the date of issue and may be renewed at any Smathers Libraries circulation desk.

Computers must be used in accordance with library and university policy and procedures listed above. Any violation may lead to loss of these privileges. For your protection, report any lost or stolen card immediately and ensure you log-off your account at the end of use to protect your privacy.

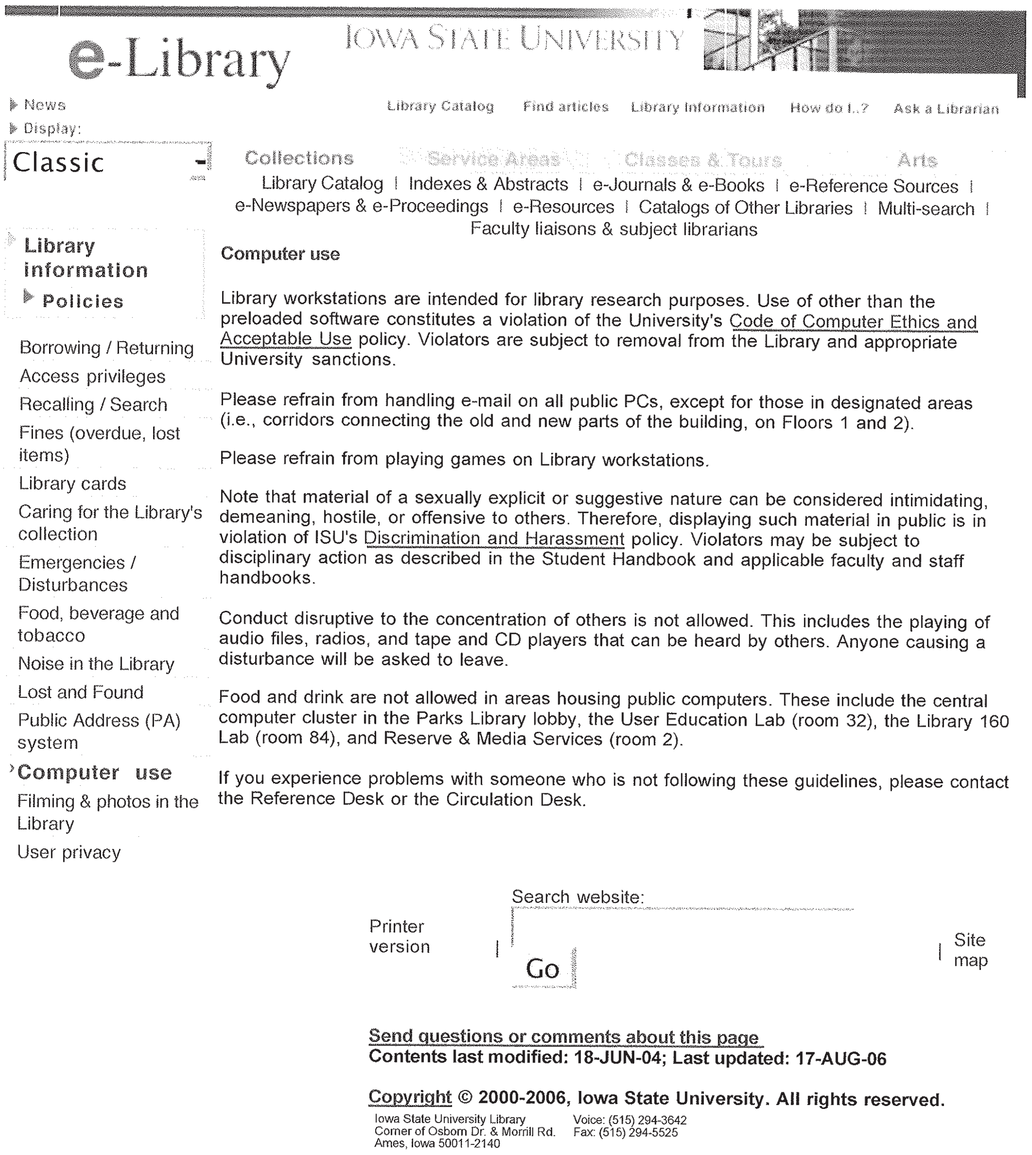
George A. Smathers Libraries, University of Florida. Adopted 03/31/99. Revised 04/03/06

Staff Web | Staff Directory | Departments | Privacy Policy

Send suggestions and comments to the library web manager.
© 1999 - 2006 University of Florida George A. Smathers Libraries.
All rights reserved
Acceptable Use, Copyright, and Disclaimer Statement
Last updated June 20, 2006 - flm

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

http://www.lib.iastate.edu/cfora/generic.cfm?cat=gen_libinfo&navid=11060&parent=3033&disp=classic&pagemode=


e-Library
IOWA STATE UNIVERSITY
News
Display:
Classic
Library Catalog
Find articles
Library Information
How do I..?
Ask a Librarian
Collections
Service Areas
Classes & Tours
Arts
Library Catalog | Indexes & Abstracts | e-Journals & e-Books | e-Reference Sources | e-Newspapers & e-Proceedings | e-Resources | Catalogs of Other Libraries | Multi-search | Faculty liaisons & subject librarians
Library information
Policies
Borrowing / Returning
Access privileges
Recalling / Search
Fines (overdue, lost items)
Library cards
Caring for the Library's collection
Emergencies / Disturbances
Food, beverage and tobacco
Noise in the Library
Lost and Found
Public Address (PA) system
Computer use
Filming & photos in the Library
User privacy
Printer version
Search website:
Go
Site map

Computer use

Library workstations are intended for library research purposes. Use of other than the preloaded software constitutes a violation of the University's Code of Computer Ethics and Acceptable Use policy. Violators are subject to removal from the Library and appropriate University sanctions.

Please refrain from handling e-mail on all public PCs, except for those in designated areas (i.e., corridors connecting the old and new parts of the building, on Floors 1 and 2).

Please refrain from playing games on Library workstations.

Note that material of a sexually explicit or suggestive nature can be considered intimidating, demeaning, hostile, or offensive to others. Therefore, displaying such material in public is in violation of ISU's Discrimination and Harassment policy. Violators may be subject to disciplinary action as described in the Student Handbook and applicable faculty and staff handbooks.

Conduct disruptive to the concentration of others is not allowed. This includes the playing of audio files, radios, and tape and CD players that can be heard by others. Anyone causing a disturbance will be asked to leave.

Food and drink are not allowed in areas housing public computers. These include the central computer cluster in the Parks Library lobby, the User Education Lab (room 32), the Library 160 Lab (room 84), and Reserve & Media Services (room 2).

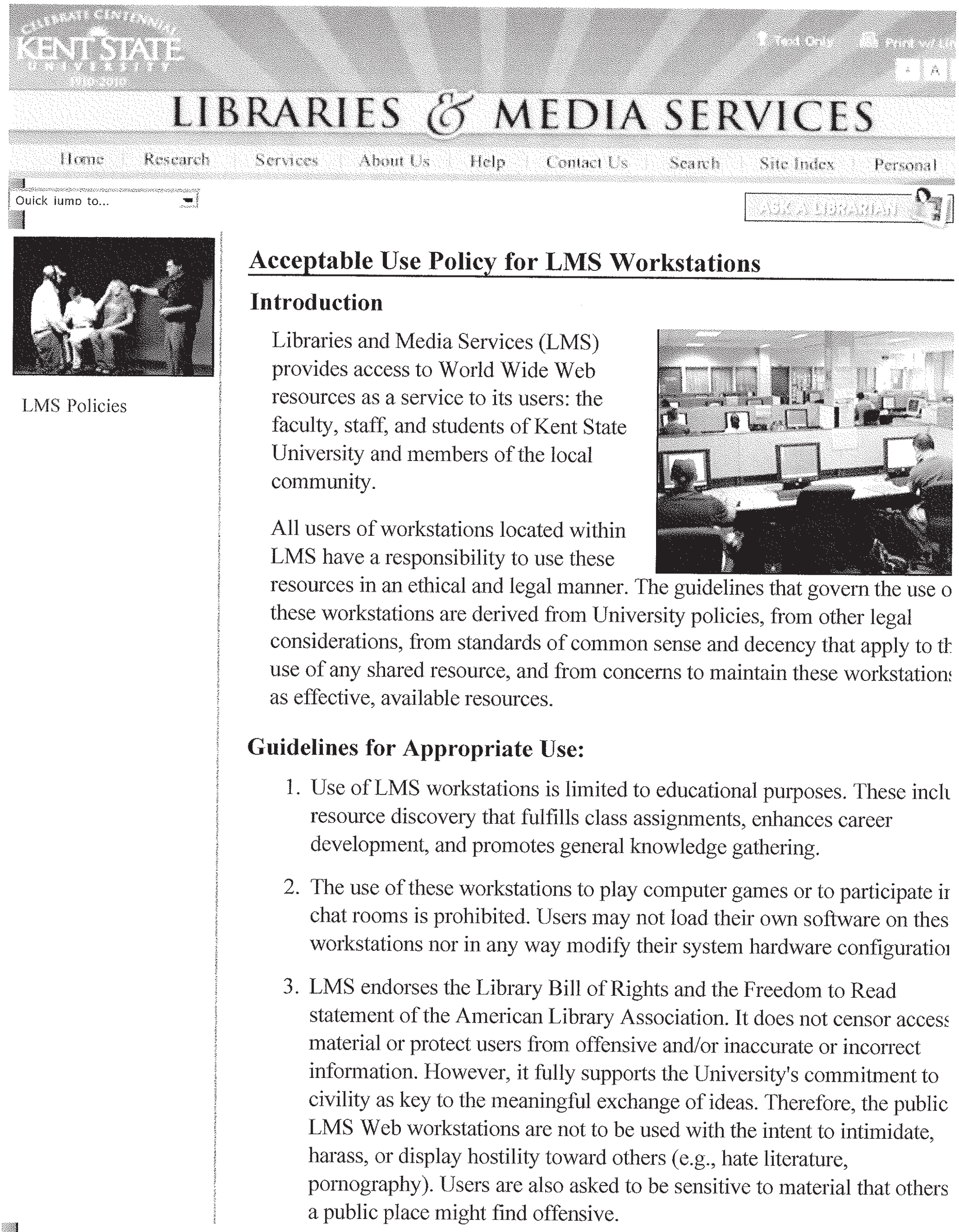
If you experience problems with someone who is not following these guidelines, please contact the Reference Desk or the Circulation Desk.

Send questions or comments about this page
Contents last modified: 18-JUN-04; Last updated: 17-AUG-06

Iowa State University Library
Corner of Osborn Dr. & Morrill Rd.
Ames, Iowa 50011-2140

Voice: (515) 294-3642
Fax: (515) 294-5525

http://www.library.kent.edu/page/10509



LMS Policies

Acceptable Use Policy for LMS Workstations

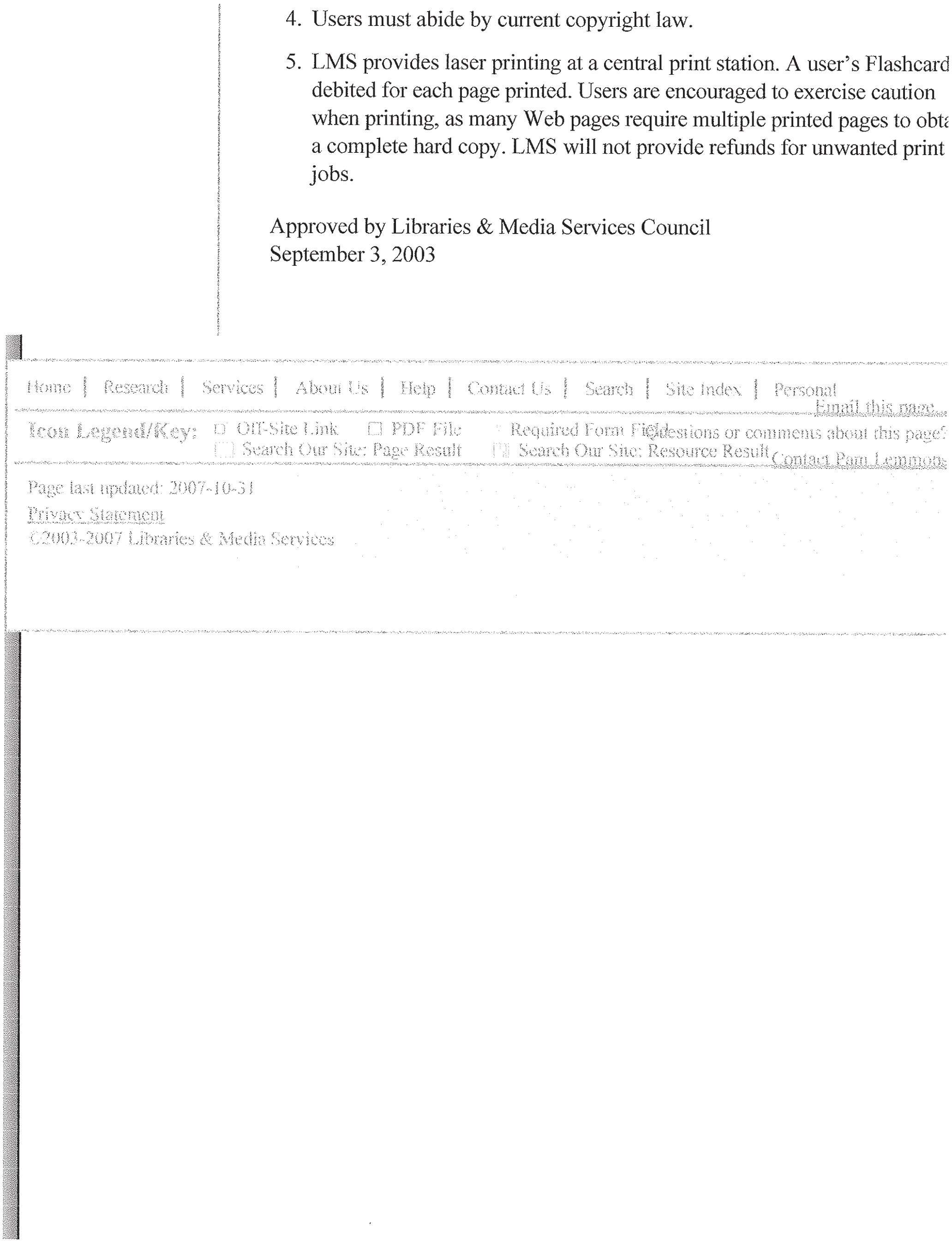
Introduction

Libraries and Media Services (LMS) provides access to World Wide Web resources as a service to its users: the faculty, staff, and students of Kent State University and members of the local community.

All users of workstations located within LMS have a responsibility to use these resources in an ethical and legal manner. The guidelines that govern the use o these workstations are derived from University policies, from other legal considerations, from standards of common sense and decency that apply to th use of any shared resource, and from concerns to maintain these workstations as effective, available resources.

Guidelines for Appropriate Use:

1. Use of LMS workstations is limited to educational purposes. These incl resource discovery that fulfills class assignments, enhances career development, and promotes general knowledge gathering.
2. The use of these workstations to play computer games or to participate ir chat rooms is prohibited. Users may not load their own software on thes workstations nor in any way modify their system hardware configuratio
3. LMS endorses the Library Bill of Rights and the Freedom to Read statement of the American Library Association. It does not censor access material or protect users from offensive and/or inaccurate or incorrect information. However, it fully supports the University's commitment to civility as key to the meaningful exchange of ideas. Therefore, the public LMS Web workstations are not to be used with the intent to intimidate, harass, or display hostility toward others (e.g., hate literature, pornography). Users are also asked to be sensitive to material that others a public place might find offensive.



4. Users must abide by current copyright law.
5. LMS provides laser printing at a central print station. A user's Flashcard debited for each page printed. Users are encouraged to exercise caution when printing, as many Web pages require multiple printed pages to obta a complete hard copy. LMS will not provide refunds for unwanted print jobs.

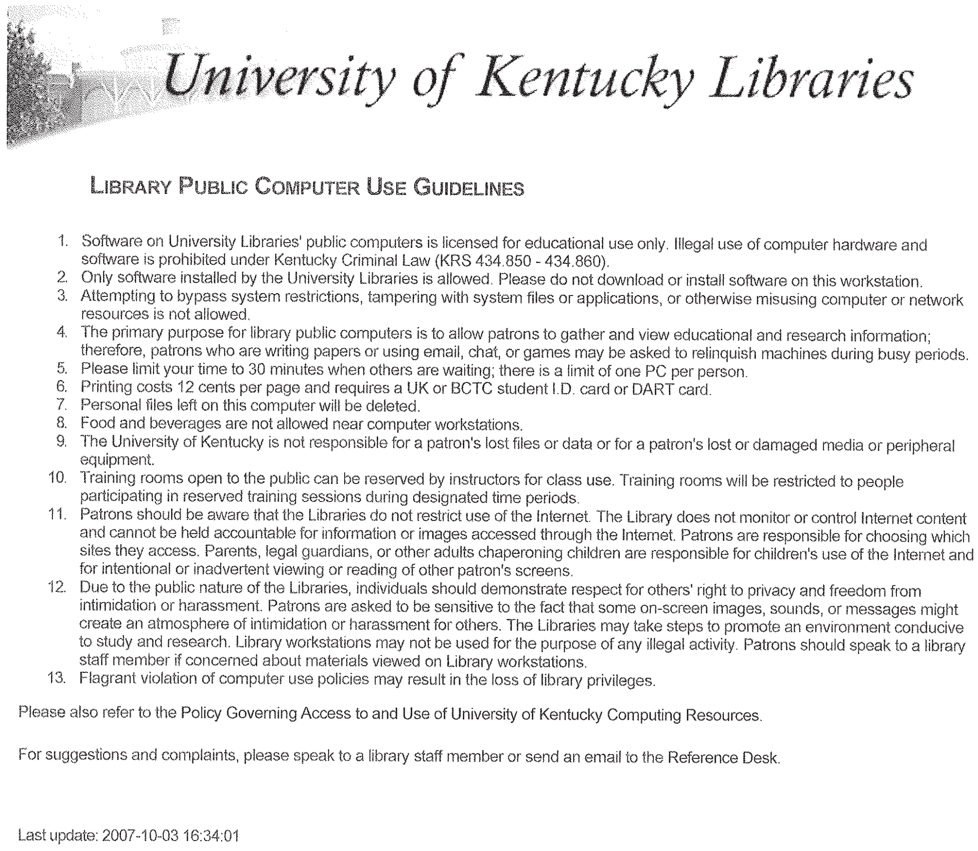
Approved by Libraries & Media Services Council
September 3, 2003

Home | Research | Services | About Us | Help | Contact Us | Search | Site Index | Personal
Email this page...
Icon Legend/Key: □ Off-Site Link □ PDF File * Required Form Field
□ Search Our Site: Page Result □ Search Our Site: Resource Result
Questions or comments about this page?
Contact Pam Lemmons

Page last updated: 2007-10-31

Privacy Statement

http://www.uky.edu/Libraries/page.php?lweb_id=288



University of Kentucky Libraries

Library Public Computer Use Guidelines

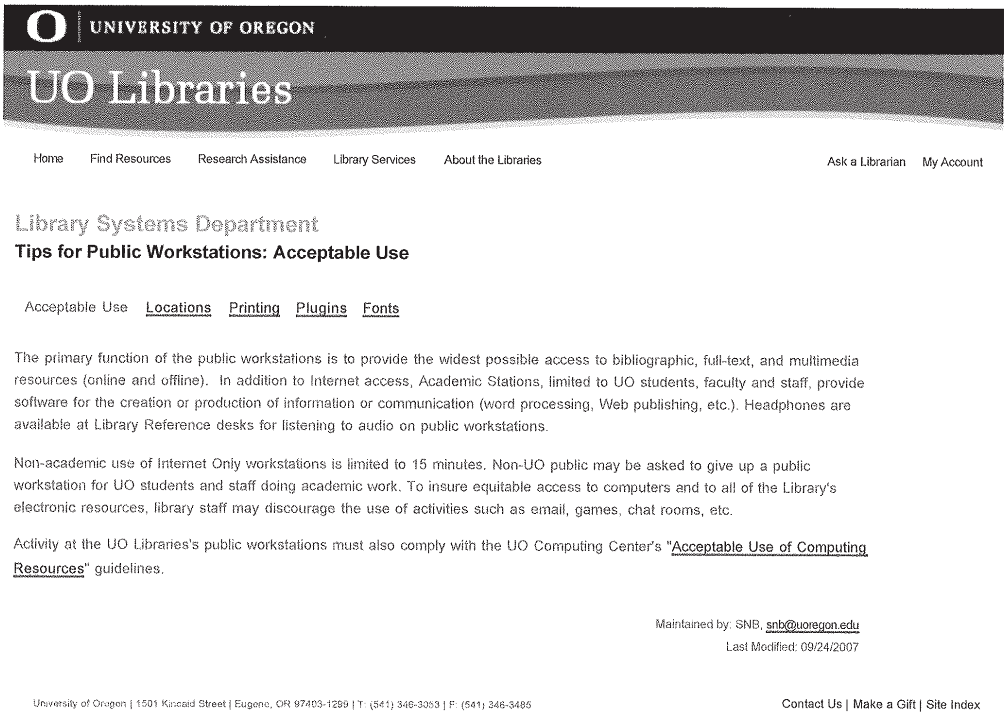
1. Software on University Libraries' public computers is licensed for educational use only. Illegal use of computer hardware and software is prohibited under Kentucky Criminal Law (KRS 434.850 - 434.860).
2. Only software installed by the University Libraries is allowed. Please do not download or install software on this workstation.
3. Attempting to bypass system restrictions, tampering with system files or applications, or otherwise misusing computer or network resources is not allowed.
4. The primary purpose for library public computers is to allow patrons to gather and view educational and research information; therefore, patrons who are writing papers or using email, chat, or games may be asked to relinquish machines during busy periods.
5. Please limit your time to 30 minutes when others are waiting; there is a limit of one PC per person.
6. Printing costs 12 cents per page and requires a UK or BCTC student I.D. card or DART card.
7. Personal files left on this computer will be deleted.
8. Food and beverages are not allowed near computer workstations.
9. The University of Kentucky is not responsible for a patron's lost files or data or for a patron's lost or damaged media or peripheral equipment.
10. Training rooms open to the public can be reserved by instructors for class use. Training rooms will be restricted to people participating in reserved training sessions during designated time periods.
11. Patrons should be aware that the Libraries do not restrict use of the Internet. The Library does not monitor or control Internet content and cannot be held accountable for information or images accessed through the Internet. Patrons are responsible for choosing which sites they access. Parents, legal guardians, or other adults chaperoning children are responsible for children's use of the Internet and for intentional or inadvertent viewing or reading of other patron's screens.
12. Due to the public nature of the Libraries, individuals should demonstrate respect for others' right to privacy and freedom from intimidation or harassment. Patrons are asked to be sensitive to the fact that some on-screen images, sounds, or messages might create an atmosphere of intimidation or harassment for others. The Libraries may take steps to promote an environment conducive to study and research. Library workstations may not be used for the purpose of any illegal activity. Patrons should speak to a library staff member if concerned about materials viewed on Library workstations.
13. Flagrant violation of computer use policies may result in the loss of library privileges.

Please also refer to the Policy Governing Access to and Use of University of Kentucky Computing Resources.

For suggestions and complaints, please speak to a library staff member or send an email to the Reference Desk.

Last update: 2007-10-03 16:34:01

http://libweb.uoregon.edu/systems/pubinfo/use.html



Library Systems Department

Tips for Public Workstations: Acceptable Use

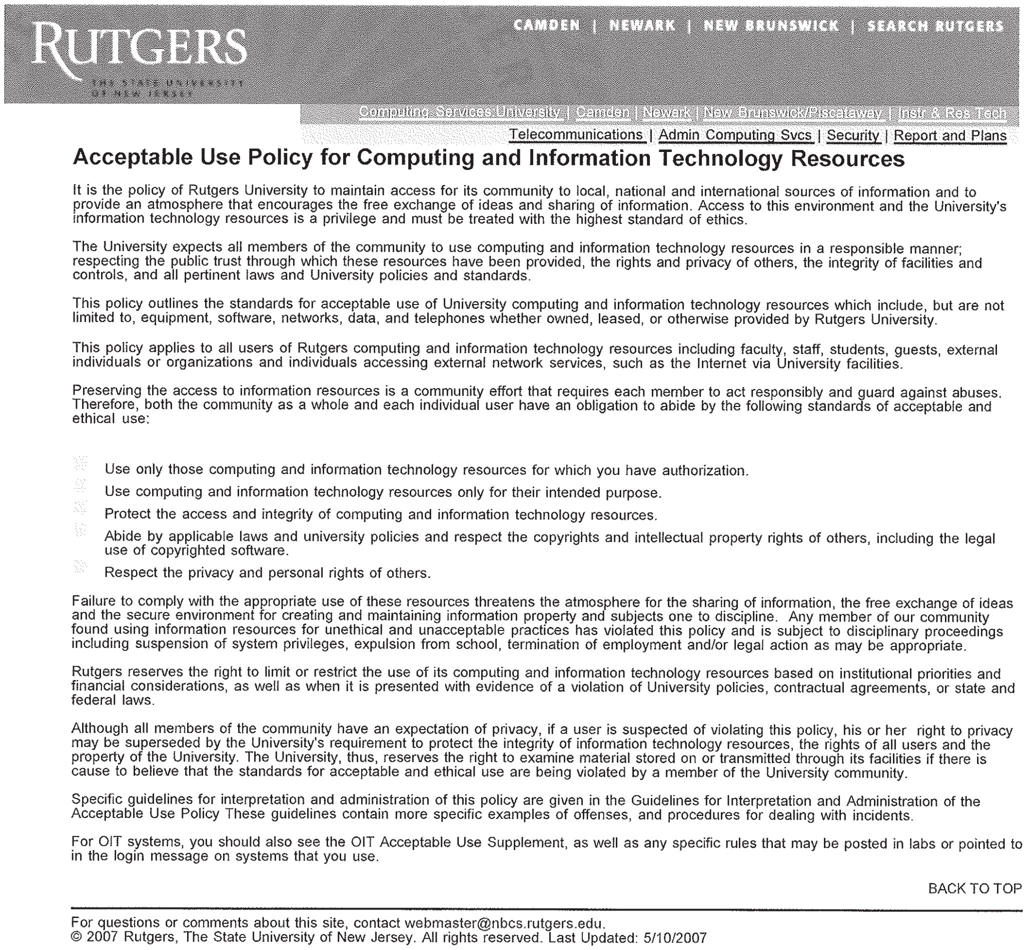
The primary function of the public workstations is to provide the widest possible access to bibliographic, full-text, and multimedia resources (online and offline). In addition to Internet access, Academic Stations, limited to UO students, faculty and staff, provide software for the creation or production of information or communication (word processing, Web publishing, etc.). Headphones are available at Library Reference desks for listening to audio on public workstations.

Non-academic use of Internet Only workstations is limited to 15 minutes. Non-UO public may be asked to give up a public workstation for UO students and staff doing academic work. To insure equitable access to computers and to all of the Library's electronic resources, library staff may discourage the use of activities such as email, games, chat rooms, etc.

Activity at the UO Libraries's public workstations must also comply with the UO Computing Center's "Acceptable Use of Computing Resources" guidelines.

Maintained by: SNB, snb@uoregon.edu
Last Modified: 09/24/2007

University of Oregon | 1501 Kincaid Street | Eugene, OR 97403-1299 | T: (541) 346-3053 | F: (541) 346-3485 http://oit.rutgers.edu/acceptable-use.html


RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY
CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS
Computing Services University | Camden | Newark | New Brunswick/Piscataway | Instr & Res Tech
Telecommunications | Admin Computing Svcs | Security | Report and Plans

Acceptable Use Policy for Computing and Information Technology Resources

It is the policy of Rutgers University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Access to this environment and the University's information technology resources is a privilege and must be treated with the highest standard of ethics.

The University expects all members of the community to use computing and information technology resources in a responsible manner; respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, and all pertinent laws and University policies and standards.

This policy outlines the standards for acceptable use of University computing and information technology resources which include, but are not limited to, equipment, software, networks, data, and telephones whether owned, leased, or otherwise provided by Rutgers University.

This policy applies to all users of Rutgers computing and information technology resources including faculty, staff, students, guests, external individuals or organizations and individuals accessing external network services, such as the Internet via University facilities.

Preserving the access to information resources is a community effort that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those computing and information technology resources for which you have authorization.
- Use computing and information technology resources only for their intended purpose.
- Protect the access and integrity of computing and information technology resources.
- Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
- Respect the privacy and personal rights of others.

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information property and subjects one to discipline. Any member of our community found using information resources for unethical and unacceptable practices has violated this policy and is subject to disciplinary proceedings including suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate.

Rutgers reserves the right to limit or restrict the use of its computing and information technology resources based on institutional priorities and financial considerations, as well as when it is presented with evidence of a violation of University policies, contractual agreements, or state and federal laws.

Although all members of the community have an expectation of privacy, if a user is suspected of violating this policy, his or her right to privacy may be superseded by the University's requirement to protect the integrity of information technology resources, the rights of all users and the property of the University. The University, thus, reserves the right to examine material stored on or transmitted through its facilities if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the University community.

Specific guidelines for interpretation and administration of this policy are given in the Guidelines for Interpretation and Administration of the Acceptable Use Policy These guidelines contain more specific examples of offenses, and procedures for dealing with incidents.

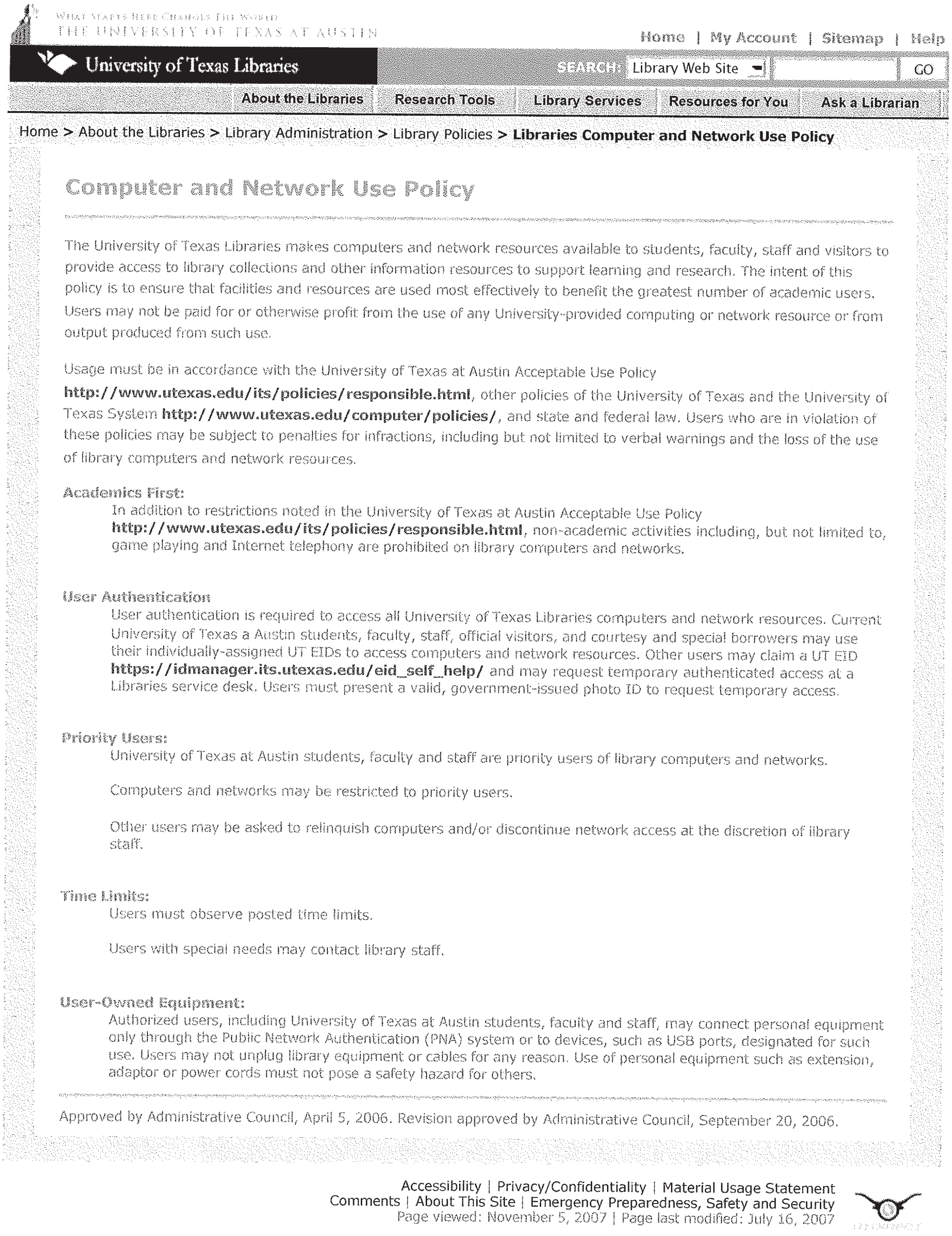
For OIT systems, you should also see the OIT Acceptable Use Supplement, as well as any specific rules that may be posted in labs or pointed to in the login message on systems that you use.

BACK TO TOP

For questions or comments about this site, contact webmaster@nbcs.rutgers.edu.

Last Updated: 5/10/2007

http://www.lib.utexas.edu/vprovost/policies/computer-use-policy.html


What Starts Here Changes The World
The University of Texas at Austin
Home | My Account | Sitemap | Help
University of Texas Libraries
SEARCH: Library Web Site
GO
About the Libraries
Research Tools
Library Services
Resources for You
Ask a Librarian
Home > About the Libraries > Library Administration > Library Policies > Libraries Computer and Network Use Policy

Computer and Network Use Policy

The University of Texas Libraries makes computers and network resources available to students, faculty, staff and visitors to provide access to library collections and other information resources to support learning and research. The intent of this policy is to ensure that facilities and resources are used most effectively to benefit the greatest number of academic users. Users may not be paid for or otherwise profit from the use of any University-provided computing or network resource or from output produced from such use.

Usage must be in accordance with the University of Texas at Austin Acceptable Use Policy **http://www.utexas.edu/its/policies/responsible.html**, other policies of the University of Texas and the University of Texas System **http://www.utexas.edu/computer/policies/**, and state and federal law. Users who are in violation of these policies may be subject to penalties for infractions, including but not limited to verbal warnings and the loss of the use of library computers and network resources.

Academics First:

In addition to restrictions noted in the University of Texas at Austin Acceptable Use Policy **http://www.utexas.edu/its/policies/responsible.html**, non-academic activities including, but not limited to, game playing and Internet telephony are prohibited on library computers and networks.

User Authentication

User authentication is required to access all University of Texas Libraries computers and network resources. Current University of Texas a Austin students, faculty, staff, official visitors, and courtesy and special borrowers may use their individually-assigned UT EIDs to access computers and network resources. Other users may claim a UT EID **https://idmanager.its.utexas.edu/eid_self_help/** and may request temporary authenticated access at a Libraries service desk. Users must present a valid, government-issued photo ID to request temporary access.

Priority Users:

University of Texas at Austin students, faculty and staff are priority users of library computers and networks.

Computers and networks may be restricted to priority users.

Other users may be asked to relinquish computers and/or discontinue network access at the discretion of library staff.

Time Limits:

Users must observe posted time limits.

Users with special needs may contact library staff.

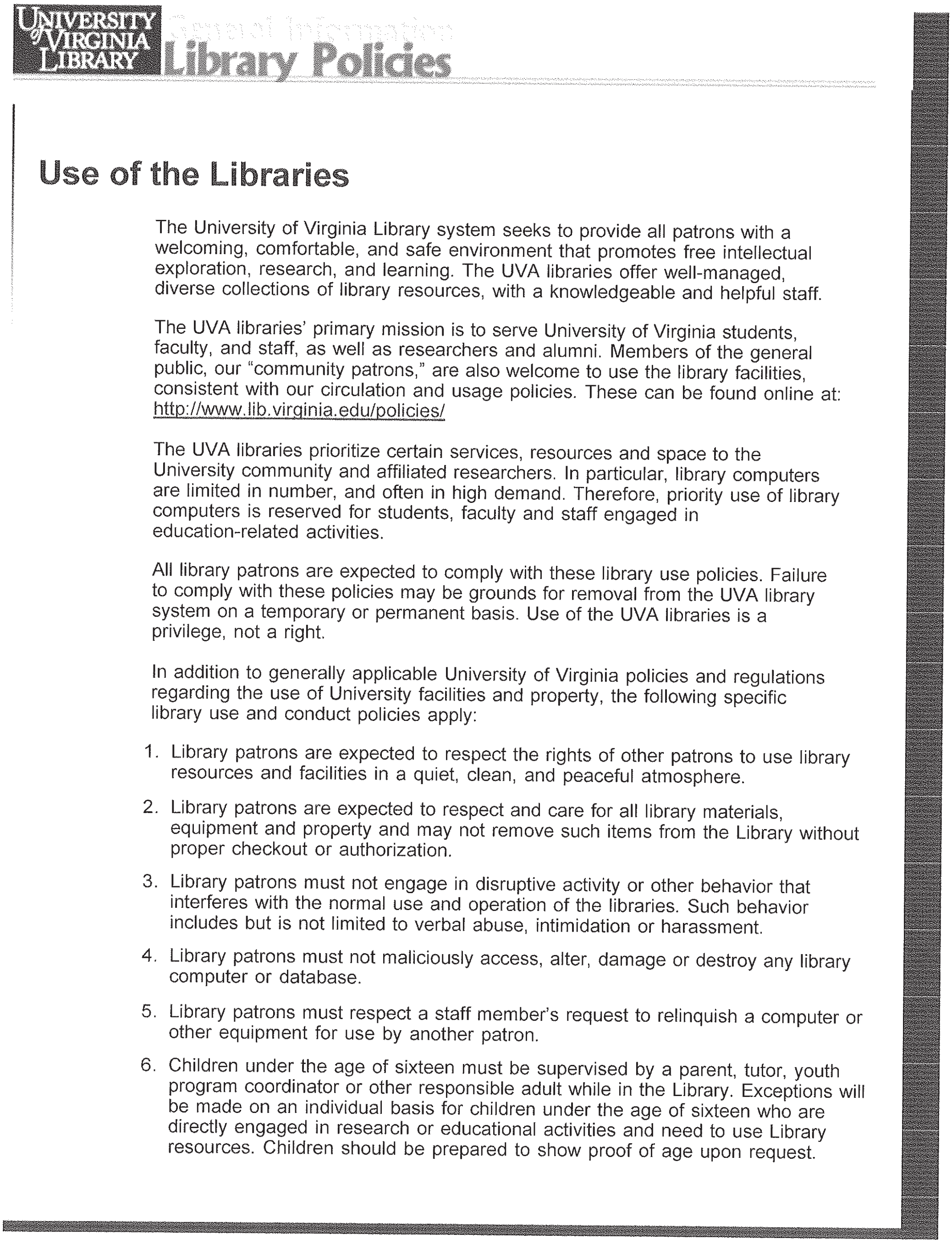
User-Owned Equipment:

Authorized users, including University of Texas at Austin students, faculty and staff, may connect personal equipment only through the Public Network Authentication (PNA) system or to devices, such as USB ports, designated for such use. Users may not unplug library equipment or cables for any reason. Use of personal equipment such as extension, adaptor or power cords must not pose a safety hazard for others.

Approved by Administrative Council, April 5, 2006. Revision approved by Administrative Council, September 20, 2006.

Accessibility | Privacy/Confidentiality | Material Usage Statement
Comments | About This Site | Emergency Preparedness, Safety and Security

Page viewed: November 5, 2007 | Page last modified: July 16, 2007 http://www.lib.virginia.edu/policies/use.html



University of Virginia Library

General Information

Library Policies

Use of the Libraries

The University of Virginia Library system seeks to provide all patrons with a welcoming, comfortable, and safe environment that promotes free intellectual exploration, research, and learning. The UVA libraries offer well-managed, diverse collections of library resources, with a knowledgeable and helpful staff.

The UVA libraries' primary mission is to serve University of Virginia students, faculty, and staff, as well as researchers and alumni. Members of the general public, our "community patrons," are also welcome to use the library facilities, consistent with our circulation and usage policies. These can be found online at: http://www.lib.virginia.edu/policies/

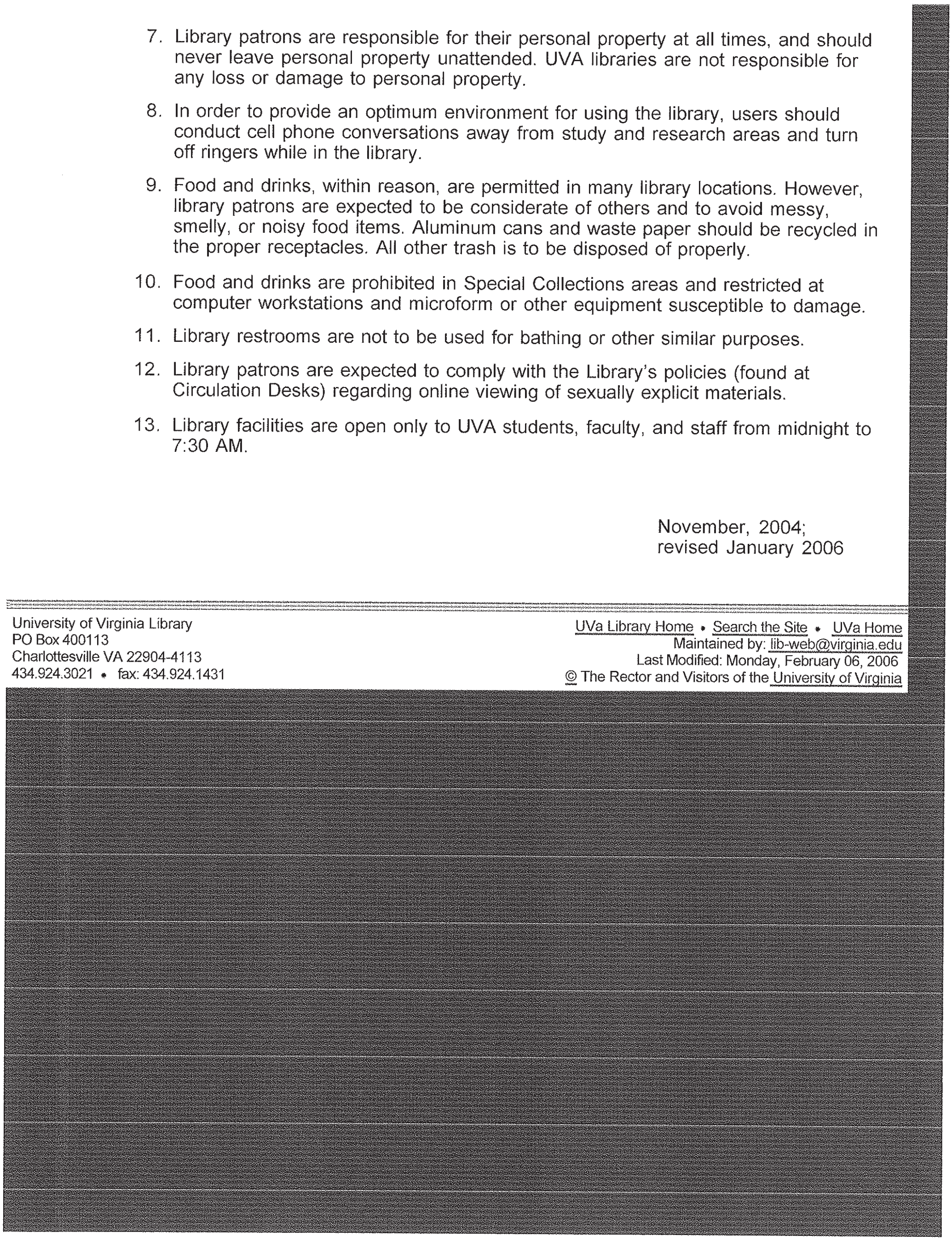
The UVA libraries prioritize certain services, resources and space to the University community and affiliated researchers. In particular, library computers are limited in number, and often in high demand. Therefore, priority use of library computers is reserved for students, faculty and staff engaged in education-related activities.

All library patrons are expected to comply with these library use policies. Failure to comply with these policies may be grounds for removal from the UVA library system on a temporary or permanent basis. Use of the UVA libraries is a privilege, not a right.

In addition to generally applicable University of Virginia policies and regulations regarding the use of University facilities and property, the following specific library use and conduct policies apply:

1. Library patrons are expected to respect the rights of other patrons to use library resources and facilities in a quiet, clean, and peaceful atmosphere.
2. Library patrons are expected to respect and care for all library materials, equipment and property and may not remove such items from the Library without proper checkout or authorization.
3. Library patrons must not engage in disruptive activity or other behavior that interferes with the normal use and operation of the libraries. Such behavior includes but is not limited to verbal abuse, intimidation or harassment.
4. Library patrons must not maliciously access, alter, damage or destroy any library computer or database.
5. Library patrons must respect a staff member's request to relinquish a computer or other equipment for use by another patron.
6. Children under the age of sixteen must be supervised by a parent, tutor, youth program coordinator or other responsible adult while in the Library. Exceptions will be made on an individual basis for children under the age of sixteen who are directly engaged in research or educational activities and need to use Library resources. Children should be prepared to show proof of age upon request.

http://www.lib.virginia.edu/policies/use.html



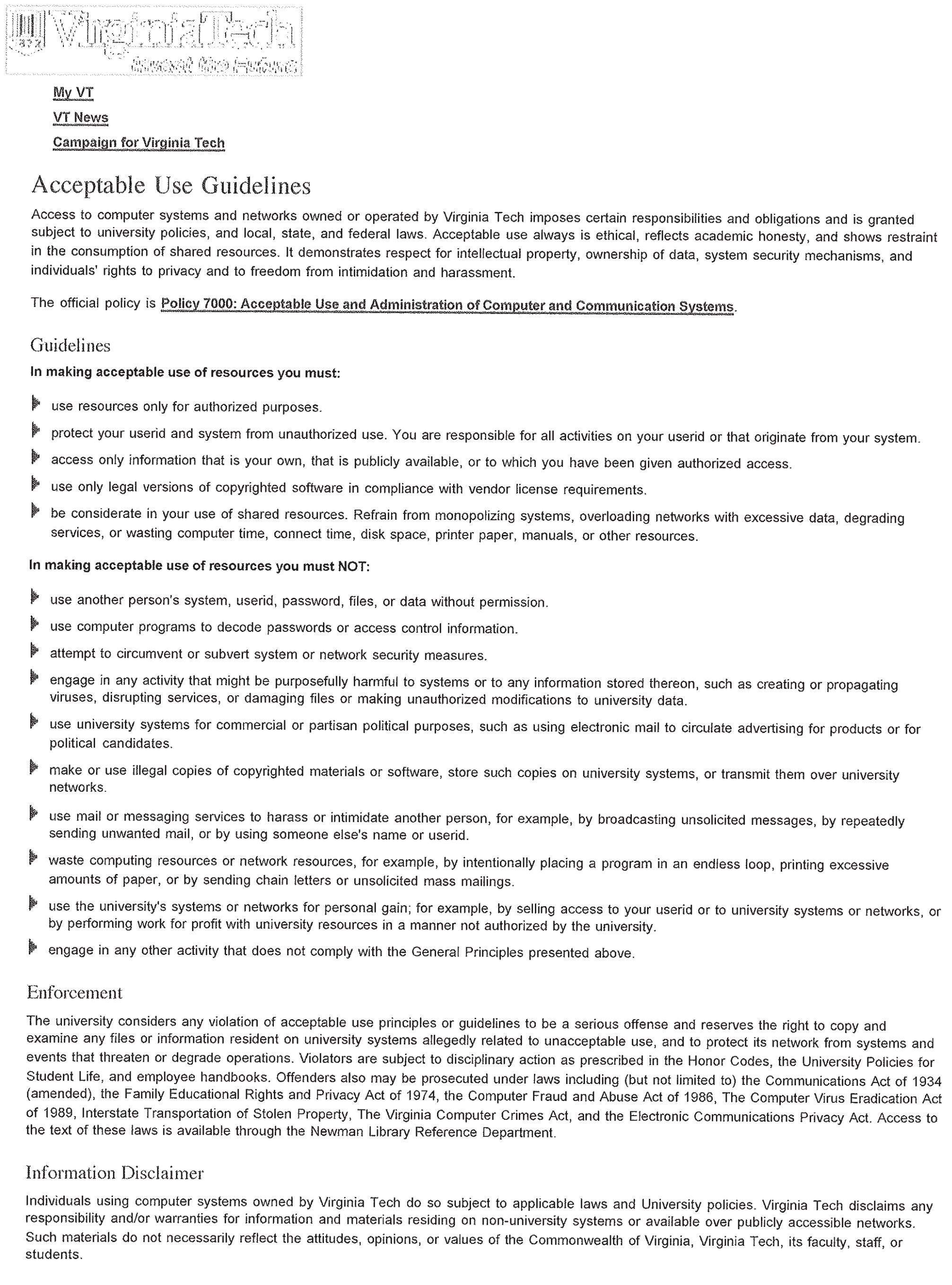
7. Library patrons are responsible for their personal property at all times, and should never leave personal property unattended. UVA libraries are not responsible for any loss or damage to personal property.
8. In order to provide an optimum environment for using the library, users should conduct cell phone conversations away from study and research areas and turn off ringers while in the library.
9. Food and drinks, within reason, are permitted in many library locations. However, library patrons are expected to be considerate of others and to avoid messy, smelly, or noisy food items. Aluminum cans and waste paper should be recycled in the proper receptacles. All other trash is to be disposed of properly.
10. Food and drinks are prohibited in Special Collections areas and restricted at computer workstations and microform or other equipment susceptible to damage.
11. Library restrooms are not to be used for bathing or other similar purposes.
12. Library patrons are expected to comply with the Library's policies (found at Circulation Desks) regarding online viewing of sexually explicit materials.
13. Library facilities are open only to UVA students, faculty, and staff from midnight to 7:30 AM.

November, 2004;
revised January 2006

University of Virginia Library
PO Box 400113
Charlottesville VA 22904-4113
434.924.3021 • fax: 434.924.1431

UVa Library Home • Search the Site • UVa Home
Maintained by: lib-web@virginia.edu
Last Modified: Monday, February 06, 2006

http://www.vt.edu/acceptable_use.php



My VT

VT News

Campaign for Virginia Tech

Acceptable Use Guidelines

Access to computer systems and networks owned or operated by Virginia Tech imposes certain responsibilities and obligations and is granted subject to university policies, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

The official policy is **Policy 7000: Acceptable Use and Administration of Computer and Communication Systems**.

Guidelines

In making acceptable use of resources you must:

- use resources only for authorized purposes.
- protect your userid and system from unauthorized use. You are responsible for all activities on your userid or that originate from your system.
- access only information that is your own, that is publicly available, or to which you have been given authorized access.
- use only legal versions of copyrighted software in compliance with vendor license requirements.
- be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

In making acceptable use of resources you must NOT:

- use another person's system, userid, password, files, or data without permission.
- use computer programs to decode passwords or access control information.
- attempt to circumvent or subvert system or network security measures.
- engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to university data.
- use university systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
- use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or userid.
- waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- use the university's systems or networks for personal gain; for example, by selling access to your userid or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the university.
- engage in any other activity that does not comply with the General Principles presented above.

Enforcement

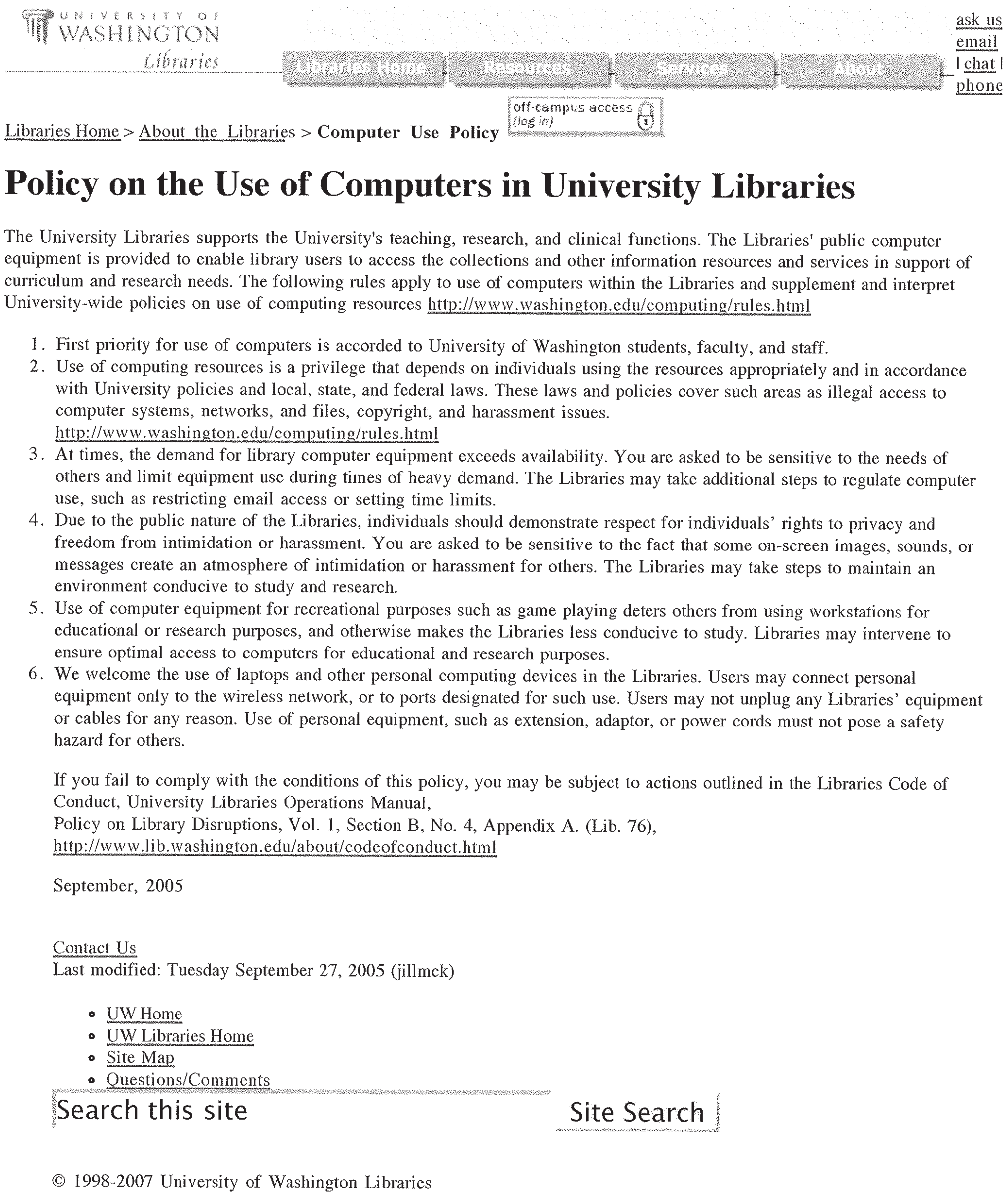
The university considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on university systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to disciplinary action as prescribed in the Honor Codes, the University Policies for Student Life, and employee handbooks. Offenders also may be prosecuted under laws including (but not limited to) the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, The Virginia Computer Crimes Act, and the Electronic Communications Privacy Act. Access to the text of these laws is available through the Newman Library Reference Department.

Information Disclaimer

Individuals using computer systems owned by Virginia Tech do so subject to applicable laws and University policies. Virginia Tech disclaims any responsibility and/or warranties for information and materials residing on non-university systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the Commonwealth of Virginia, Virginia Tech, its faculty, staff, or students.

UNIVERSITY OF WASHINGTON

http://www.lib.washington.edu/about/computerusepolicy.html



UNIVERSITY OF WASHINGTON Libraries
Libraries Home
Resources
Services
About
ask us
email
| chat |
phone
off-campus access (log in)

Libraries Home > About the Libraries > **Computer Use Policy**

Policy on the Use of Computers in University Libraries

The University Libraries supports the University's teaching, research, and clinical functions. The Libraries' public computer equipment is provided to enable library users to access the collections and other information resources and services in support of curriculum and research needs. The following rules apply to use of computers within the Libraries and supplement and interpret University-wide policies on use of computing resources http://www.washington.edu/computing/rules.html

1. First priority for use of computers is accorded to University of Washington students, faculty, and staff.
2. Use of computing resources is a privilege that depends on individuals using the resources appropriately and in accordance with University policies and local, state, and federal laws. These laws and policies cover such areas as illegal access to computer systems, networks, and files, copyright, and harassment issues. http://www.washington.edu/computing/rules.html
3. At times, the demand for library computer equipment exceeds availability. You are asked to be sensitive to the needs of others and limit equipment use during times of heavy demand. The Libraries may take additional steps to regulate computer use, such as restricting email access or setting time limits.
4. Due to the public nature of the Libraries, individuals should demonstrate respect for individuals' rights to privacy and freedom from intimidation or harassment. You are asked to be sensitive to the fact that some on-screen images, sounds, or messages create an atmosphere of intimidation or harassment for others. The Libraries may take steps to maintain an environment conducive to study and research.
5. Use of computer equipment for recreational purposes such as game playing deters others from using workstations for educational or research purposes, and otherwise makes the Libraries less conducive to study. Libraries may intervene to ensure optimal access to computers for educational and research purposes.
6. We welcome the use of laptops and other personal computing devices in the Libraries. Users may connect personal equipment only to the wireless network, or to ports designated for such use. Users may not unplug any Libraries' equipment or cables for any reason. Use of personal equipment, such as extension, adaptor, or power cords must not pose a safety hazard for others.

If you fail to comply with the conditions of this policy, you may be subject to actions outlined in the Libraries Code of Conduct, University Libraries Operations Manual,
Policy on Library Disruptions, Vol. 1, Section B, No. 4, Appendix A. (Lib. 76),
http://www.lib.washington.edu/about/codeofconduct.html

September, 2005

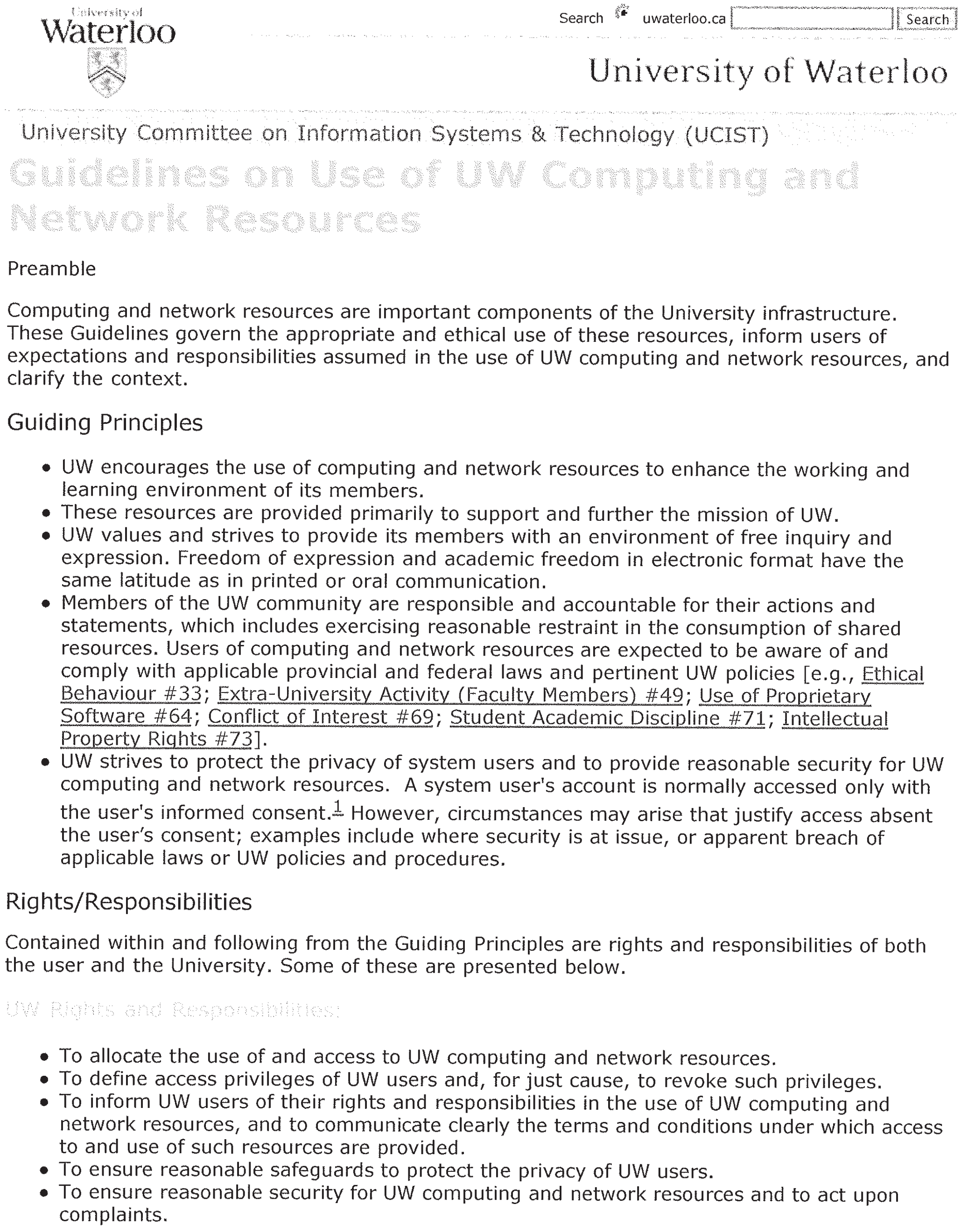
Contact Us
Last modified: Tuesday September 27, 2005 (jillmck)

- UW Home
- UW Libraries Home
- Site Map
- Questions/Comments

Search this site Site Search

UNIVERSITY OF WATERLOO

http://www.adm.uwaterloo.ca/infocist/use2006.htm



University of Waterloo

University Committee on Information Systems & Technology (UCIST)

Guidelines on Use of UW Computing and Network Resources

Preamble

Computing and network resources are important components of the University infrastructure. These Guidelines govern the appropriate and ethical use of these resources, inform users of expectations and responsibilities assumed in the use of UW computing and network resources, and clarify the context.

Guiding Principles

- UW encourages the use of computing and network resources to enhance the working and learning environment of its members.
- These resources are provided primarily to support and further the mission of UW.
- UW values and strives to provide its members with an environment of free inquiry and expression. Freedom of expression and academic freedom in electronic format have the same latitude as in printed or oral communication.
- Members of the UW community are responsible and accountable for their actions and statements, which includes exercising reasonable restraint in the consumption of shared resources. Users of computing and network resources are expected to be aware of and comply with applicable provincial and federal laws and pertinent UW policies [e.g., Ethical Behaviour #33; Extra-University Activity (Faculty Members) #49; Use of Proprietary Software #64; Conflict of Interest #69; Student Academic Discipline #71; Intellectual Property Rights #73].
- UW strives to protect the privacy of system users and to provide reasonable security for UW computing and network resources. A system user's account is normally accessed only with the user's informed consent.[1] However, circumstances may arise that justify access absent the user's consent; examples include where security is at issue, or apparent breach of applicable laws or UW policies and procedures.

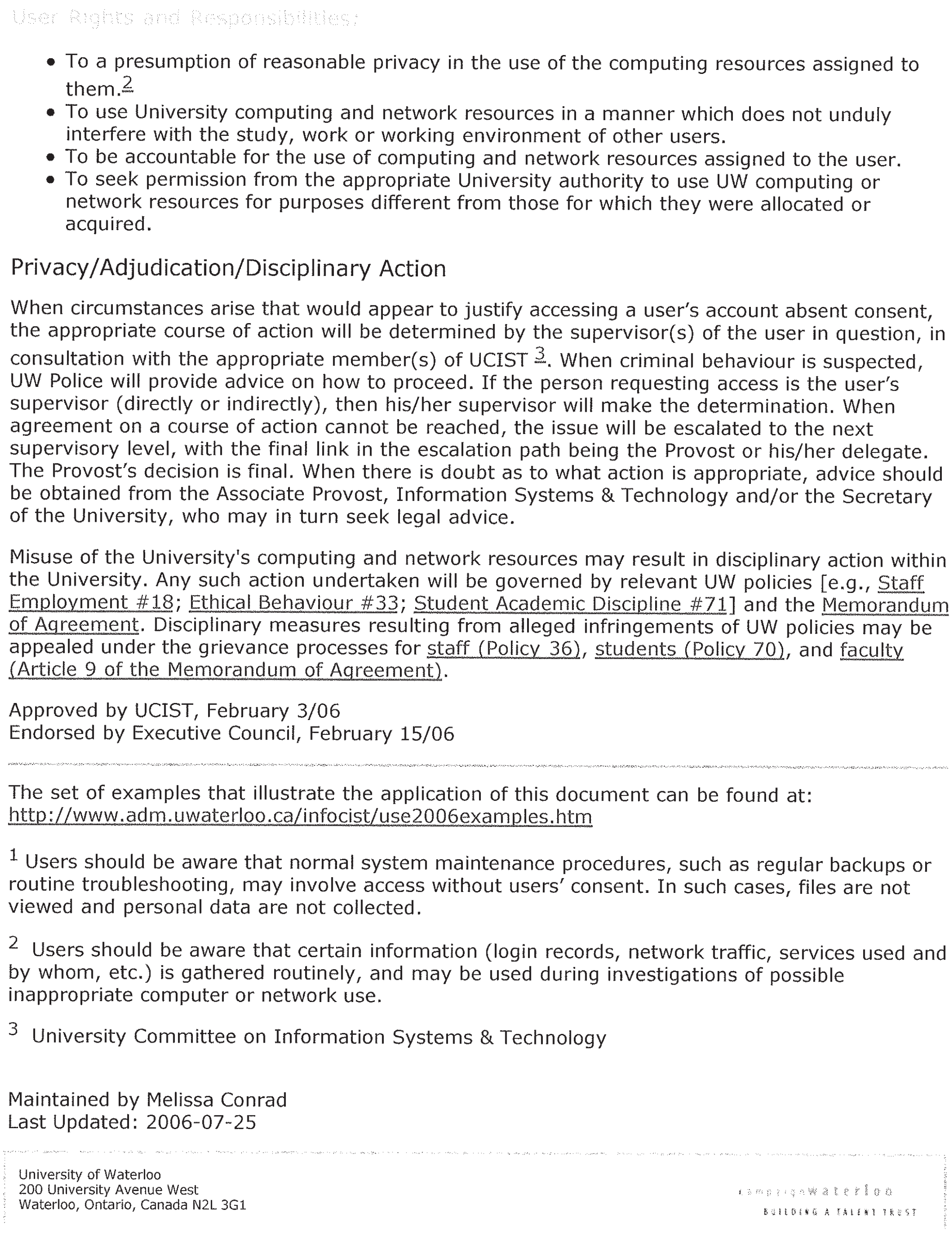
Rights/Responsibilities

Contained within and following from the Guiding Principles are rights and responsibilities of both the user and the University. Some of these are presented below.

UW Rights and Responsibilities:

- To allocate the use of and access to UW computing and network resources.
- To define access privileges of UW users and, for just cause, to revoke such privileges.
- To inform UW users of their rights and responsibilities in the use of UW computing and network resources, and to communicate clearly the terms and conditions under which access to and use of such resources are provided.
- To ensure reasonable safeguards to protect the privacy of UW users.
- To ensure reasonable security for UW computing and network resources and to act upon complaints.

http://www.adm.uwaterloo.ca/infocist/use2006.htm



User Rights and Responsibilities:

- To a presumption of reasonable privacy in the use of the computing resources assigned to them.[2]
- To use University computing and network resources in a manner which does not unduly interfere with the study, work or working environment of other users.
- To be accountable for the use of computing and network resources assigned to the user.
- To seek permission from the appropriate University authority to use UW computing or network resources for purposes different from those for which they were allocated or acquired.

Privacy/Adjudication/Disciplinary Action

When circumstances arise that would appear to justify accessing a user's account absent consent, the appropriate course of action will be determined by the supervisor(s) of the user in question, in consultation with the appropriate member(s) of UCIST [3]. When criminal behaviour is suspected, UW Police will provide advice on how to proceed. If the person requesting access is the user's supervisor (directly or indirectly), then his/her supervisor will make the determination. When agreement on a course of action cannot be reached, the issue will be escalated to the next supervisory level, with the final link in the escalation path being the Provost or his/her delegate. The Provost's decision is final. When there is doubt as to what action is appropriate, advice should be obtained from the Associate Provost, Information Systems & Technology and/or the Secretary of the University, who may in turn seek legal advice.

Misuse of the University's computing and network resources may result in disciplinary action within the University. Any such action undertaken will be governed by relevant UW policies [e.g., Staff Employment #18; Ethical Behaviour #33; Student Academic Discipline #71] and the Memorandum of Agreement. Disciplinary measures resulting from alleged infringements of UW policies may be appealed under the grievance processes for staff (Policy 36), students (Policy 70), and faculty (Article 9 of the Memorandum of Agreement).

Approved by UCIST, February 3/06
Endorsed by Executive Council, February 15/06

The set of examples that illustrate the application of this document can be found at:
http://www.adm.uwaterloo.ca/infocist/use2006examples.htm

[1] Users should be aware that normal system maintenance procedures, such as regular backups or routine troubleshooting, may involve access without users' consent. In such cases, files are not viewed and personal data are not collected.

[2] Users should be aware that certain information (login records, network traffic, services used and by whom, etc.) is gathered routinely, and may be used during investigations of possible inappropriate computer or network use.

[3] University Committee on Information Systems & Technology

Maintained by Melissa Conrad
Last Updated: 2006-07-25

University of Waterloo
200 University Avenue West
Waterloo, Ontario, Canada N2L 3G1