

NORMAN ADRIAN WIGGINS SCHOOL OF LAW, CAMPBELL UNIVERSITY COMPUTER AND NETWORK USE POLICY

This policy is intended to promote the responsible and ethical use of the computing resources of the Norman Adrian Wiggins School of Law of Campbell University. In light of the contribution that computers can make to furthering the educational and other objectives of the School of Law, it is in the best interest of the community as a whole that computing resources be used in accordance with practices which ensure that the rights of all users are protected and the goals of the School of Law are achieved.

This policy applies to all computer and computer communication facilities owned, leased, operated, or contracted by the School of Law or the University. This includes use of the law library network, the Internet server and the campus-wide network. It includes word processing equipment, microcomputers, minicomputers, mainframes and associated peripherals and software, regardless of whether used for administration, research, teaching, or other purposes. This policy also extends to any use of School of Law or University facilities to access computer facilities elsewhere.

System administrators of various on-campus and off-campus computing facilities and those responsible for access to those facilities may promulgate additional regulations to control their use, if not inconsistent with this policy. System administrators are responsible for publicizing any additional regulations concerning the authorized and appropriate use of the equipment for which they are responsible.

Basic Principles

As in all aspects of University life, a user of computing facilities should act honorably and in a manner consistent with ordinary ethical obligations. Cheating, stealing, making false or deceiving statements, plagiarism, vandalism, and harassment are just as wrong when done in the context of computing as they are in all other aspects of University conduct. Individuals should use only those computing facilities they have been authorized through ordinary channels to use. They should use these facilities:

- ▶ in a manner consistent with the terms
- ▶ under which they were granted access to them;
- ▶ in a way that respects the rights and
- ▶ privacy of other users;
- ▶ so as not to interfere with or violate the
- ▶ normal, appropriate use of these facilities; and
- ▶ in a responsible and efficient manner.

Acceptable Use

Individuals who have been granted and hold an active and authorized account on a University or School of Law computer or network and abide by this policy are considered authorized users.

Authorized use is that which is consistent with the academic, research and service goals of this institution and falls within the guidelines of this policy and the policy of the University which states that property owned by the institution shall be used only for institutional purposes.

Users are expected to respect the right to privacy of other individuals on the network. Do not go browsing around in someone's files even if security permissions permit. This is analogous to condoning someone rifling around on your desk or in your house simply because you forgot to lock your door. It is expected that explicit permission from the owner of the files be obtained before they are accessed.

Users are expected to respect the right of freedom of expression of other individuals on the network.

School of Law computer users are expected to read sign-on messages and system news for specific information such as system changes, policies and scheduled downtime.

System and network administrators may find it necessary to contact you regarding policy issues. If repeated attempts to contact an individual are unsuccessful, the system or network administrator may be forced to temporarily deactivate the account simply to compel the owner to make return contact.

Unacceptable Use

University computing resources are not to be used for commercial purposes or non-University related activities without prior written permission.

Individuals should respect the rights and privacy of other authorized users. Thus they should respect the rights of other users to security of files, confidentiality of data, and the ownership of their own work. Users should refrain from:

- ▶ using the computer access privileges of others
- ▶ accessing, copying, or modifying the files of
- ▶ others without their explicit permission;
- ▶ illegal copying of software or data; and
- ▶ harassing others in any way or interfering with their legitimate use of computing facilities.

Individuals should not attempt to interfere with the normal operation of computing systems or attempt to subvert the restrictions associated with such facilities. They should obey the regulations affecting the use of any computing facility they use.

The School of Law holds the need for academic integrity and the proper respect for ideas and authorship in the highest regard. As partners in the enterprise of scholarship, students are similarly to practice such respect.

- Do not share your account; do not give your password to anyone.

With the exception of the system administrator, every account has the same privileges. We expect each user to understand what is right and what is wrong, and we attempt to help develop this understanding. People who are not in the department may not appreciate where the limits are and do things that negatively impact our facilities. In giving a person an account, we have some expectation as to the load that account will place upon our resources and plan the development of our facilities accordingly. We cannot plan or account for unauthorized users. The person to whom we give an account is responsible for all activities that occur in that account. Some activities may call for the limitation of privileges or even the termination of the account. The

fact that the account holder did not personally conduct these activities will have no bearing on the account limitation or termination.

- Do not attempt to conceal your identity; your finger entry must contain your real name.

Mail and news postings, telnets, ftps, etc., will always be identified with Campbell University and the School of Law. As administrators of these systems, we cannot escape the responsibility for their use. Each individual account holder must share in this responsibility. If there is some reason that you personally should not be associated with an activity originating in one of our systems, there is likely good reason that the activity should not be on the system in the first place.

Anonymity is not consistent with accountability and responsibility. Runaway processes, exceptionally long jobs, lost mail, and hung connections are examples of problems that require staff intervention. If a long job is degrading system response, the staff has an obligation to terminate the job. If the job is a few minutes away from termination, however, it would be a shame to waste the run time. Only by contacting the job owner can the staff determine the best course of action. In all of the above examples, our ability to identify and contact the account holder is in everyone's best interest.

- Do not use guessable passwords.

If you make it easy for people to guess your password, you put our whole computing environment in jeopardy, not just your own files. Once through the front door, there are a number of holes that hackers can exploit to gain access to other user and system files. And this is not limited to just one machine. If you have .rhosts files, all the systems pointed to are vulnerable. Consider this to be a rule, rather than a guideline. It is policy officially accepted by the School of Law.

- Do not subvert file protections and do not access sections of the operating system not open to ordinary users.

We understand that many of our users are capable of gaining root privileges, of spoofing mail and news, and of breaking into other users' accounts. If we were to attempt to prevent this, we would have to severely restrict *everyone's* access to our systems capabilities. The fact that you are capable of doing certain things does not constitute permission to do those things. Even if your intentions are of the purest intellectual curiosity, you can break the system by trespassing in restricted areas. In the normal course of operation each user has a right to the privacy of their files. Nobody will get upset if you read his or her login file. Most people would not approve of your reading their mailbox. You're expected to use good judgment in the between areas (with the default that if you doubt, don't).

- Understand that all of our resources have limits; give up your game seat to someone who needs to do homework; use the copy machine to get 20 copies of the paper.

We have very few rules regarding the use of our facilities. We don't forbid the playing of games or the use of our systems for computing in personal interest areas. We also consider that unused resources (disk space, cycles, bandwidth, etc.) are lost forever, and might as well be used for whatever purpose. The primary missions of the department, however, are research and instruction and have priority access to the resources. When the margin becomes small enough to impact our important uses, we will ask users to free up these resources. In your desire to accomplish the immediate task, it may seem to you that printing copies instead of copying them won't make that much difference. This kind of action by 300 users over the course of the year can add up to be a significant cost. The more dollars we must spend on mundane supplies the less we have to spend on necessary things like workstations.

- When posting mail and news, remember that each submission goes out on Campbell University "letterhead."

Your freedom of expression does not extend to embarrassing the University or the School of Law. The School of Law does not censor mail or news. We reserve the right, however, to limit people's access to the mail and news systems. You have the right to say what you wish to whomever you please, but Campbell University or the School of Law does not have the obligation to provide you with the means. The Law School and Campbell University maintain some responsibility for the content and tone of the messages (as they do with letterhead paper). Usenet is coming under intense public scrutiny. We can all do our part to prevent this by making responsible and reasonable use of the net, and not engaging in illegal or unethical acts. If we get calls from postmasters at other sites indicating that one of our users is outside the normal bounds of Usenet etiquette, we will suggest to the user that they moderate their behavior, and take more assertive steps if necessary. The best defense is to not have administrators asking questions about the use of the network and the cost to the university.

Elaboration

The purpose of the following list is to aid in interpreting the principles espoused above. This list should in no way be construed as comprehensive. Examples of actions in violation of these principles are:

- ▶ copying of licensed or copyrighted software not permitted by law or by contract;
- ▶ sending harassing or libelous electronic mail;
- ▶ sending electronic mail fraudulently; for example, by misrepresenting the identity of the sender;
- ▶ using a loophole in a computer's operating system or knowledge of a privileged password to damage a computer system or to gain access to a system or resource that one is not authorized to use;
- ▶ using University computing facilities for commercial purposes without prior arrangement;
- ▶ knowingly allowing another person to use your account privileges for improper purposes;
- ▶ turning in someone else's paper or computer program as your own work;
- ▶ allowing someone else to turn in your paper
- ▶ or computer program as their own work;
- ▶ reading someone else's electronic mail
- ▶ without their permission.
- ▶ using University facilities to gain
- ▶ unauthorized access to computer
- ▶ facilities off-campus; and
- ▶ intentionally using an abnormally large amount of resources, such as processing time or disk space, without prior permission.

Computer Labs

Due to copyright guidelines, the potential of harm caused by viruses, and the need to maintain the integrity of the network, personal software is not permitted in the labs.

Malfunction of the computer equipment or software should be communicated to the lab assistant

or computer support personnel. Lab users may not attempt troubleshooting. Users must not attempt unauthorized modification of or repair to any equipment belonging to or under the control of the School of Law.

The library's policy against food, drink, and smoking strictly applies in the computer labs. Disregard of the policy will result in termination of computer lab privileges.

Disciplinary Actions

Reasonable suspicion of a violation of the principles or practices described in this policy statement may result in disciplinary action. Such action will be taken through appropriate University channels such as administrative procedures, the law school Honor Court, or other supervisory authority to which the individual is subject.

Violation of State or Federal statutes may result in civil or criminal proceedings.

Nothing in this statement diminishes the authority and responsibility of administrators of computing services to take remedial action in the case of possible abuse of computing privileges. To this end, system administrators, with due regard for the right of privacy of users and the confidentiality of their data, have the right to suspend or modify computer access privileges, examine files, passwords, accounting information, printouts, tapes, and any other material that may aid in maintaining the integrity and efficient operation of the system.

Users whose activity is viewed as a threat to the operation of a computing system, who abuse the rights of other users, or who refuse to cease improper behavior may have their use privileges revoked. In the event that access to a system is revoked, users will be provided a copy of their files.