

ACCEPTABLE USE POLICY (2003)

Applicability

Capital University computer resources are intended for University-related purposes. This policy applies to all users and all uses of those resources, whether on-campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the University or to users within specific units.

For purposes of this policy computer resources includes personal and network computer systems; hardware and physical equipment used for computing or computer communications (including but not limited to CPU-s, monitors, peripheral devices, servers, and cabling); officially licensed desktop, shared or network software; e-mail systems and software; web pages, programs or documents hosted by the University; file transfer protocol (FTP) resources; other Internet or network resources including University-provided bandwidth and disk space; voice mail; and other resources so designated by the University. Additional guidelines and information on these resources are set forth at www.capital.edu/IT, and may be amended by the University from time to time.

Policy

All users of University computer resources must:

1. comply with all federal, Ohio, and other applicable law; all applicable University rules and policies; and all applicable contracts and licenses.
2. use only those computer resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access resources does not by itself imply authorization to use them. Users are responsible for obtaining necessary authorizations.
3. respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.
4. use those resources in a manner that does not consume an unreasonable amount of those resources or interfere unreasonably with the activity of other users. The reasonableness of a use will be judged in the context of all the relevant circumstances.
5. refrain from using those resources for commercial purposes or for personal financial gain. Incidental personal use of those resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user-s job or other University responsibilities, and is otherwise in compliance with University policy. Further limits may be imposed on personal use by units or departments. Use of those

resources by faculty or staff for approved consulting or other approved professional activities is not a violation of this policy.

6. refrain from stating or implying that they speak on behalf of the University and from using University name, marks or logos without authorization to do so or outside the scope of their employment. The use of suitable disclaimers is encouraged. Authorization to use University name, marks or logos may be granted only by the Vice President for University Relations, or the VPUR's designee.

Enforcement

Users who violate this policy may be denied access to University computer resources and may be subject to other penalties and disciplinary action within and outside the University. Disciplinary action within the University will be taken pursuant to procedures applicable to the relevant user (faculty, administrator, hourly staff, student). However, the University may temporarily suspend or block access to an account prior to the initiation or completion of such procedures when it reasonably appears necessary to protect the integrity, security, or functionality of computing resources or to protect the University from liability. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

The University employs various measures to protect the security of its computer resources and of users' accounts, but cannot guarantee such security. Users should guard their passwords, change them regularly, and engage in safe computing practices.

Users should also be aware that their uses of University computer resources are not completely private. While the University does not routinely monitor individual usage of those resources, the normal operation and maintenance of those resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual users of those resources, including individual login sessions and communications, without notice, when:

- (1) the user has made them accessible to the public, as by posting a web page;
- (2) it reasonably appears necessary to do so to protect the integrity, security, or functionality of those resources;
- (3) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
- (4) there is reasonable cause to believe that the user has violated, or is violating, this policy, or it reasonably appears necessary to protect the University from liability;

(5) it is otherwise required or permitted by law and consistent with this policy.

Such individual monitoring as specified in (2) and (3) above may be authorized by the Chief Information Officer (or, in the case of the Law School, the Director of Law School Information Technology). Such individual monitoring as specified in (4) and (5) may be authorized in advance by the appropriate Vice President or Provost (or, in the case of the Law School, the Law School Dean) in consultation with University Counsel.

The University may disclose the results of any such general or individual monitoring to appropriate University personnel or law enforcement agencies, and may use those results in University disciplinary proceedings.

To the extent that a PC or network server serves as the functional equivalent of a desk drawer or file cabinet, supervisors have the same access to it for normal, non-investigative, work-related purposes (for example, to retrieve a file or document needed while the employee who maintains the file or document is away from the office). Obtaining such access is not considered monitoring for purposes of the policy and does not require the advance authorization noted above. If a supervisor discovers evidence of possible misconduct or misuse, further monitoring or investigation of those resources for purposes of dealing with the suspected misconduct or misuse does require the advance authorization noted above.

The following Statement is to be signed by all Information Technology Department employees:

IT Department Employee Certification

I understand that as a Capital University employee in the Information Technology department, the University expects of me that I will (1) not violate University policy or law, (2) report to the Chief Information Officer and University Counsel any suspected violation of University policy or law, and (3) not make any unauthorized access of, or represent to anyone that I may so access, any user e-mail or electronic record.

I further understand that the University Community's confidence in IT staff is an important trust, and I will do all I can to avoid even the appearance of impropriety in this regard. I will respect the privacy of individuals and records, and abide by all provisions of the Acceptable Use Policy.