

College of Agricultural and Life Sciences (CALs)

Information Technology Rights and Responsibilities

January 1, 2003

- I. Introduction** - Use of information technology resources at the College of Agricultural & Life Sciences (CALs), is essential to its mission to create, integrate, transfer and apply knowledge. This privilege is granted to all faculty, staff and students to ensure that the mission of the College is within reach of all of its members. With this privilege comes individual responsibility to comply with University regulations and local, state, and federal laws. Appropriate use should exercise common sense, respect an individual's privacy, reflect academic honesty, follow the mission of the institution, and adhere to local, state, and federal laws. Any additional rules or regulations may be adopted by various departments/centers to meet specific administrative or academic needs, however, any adopted requirements must also be in compliance with federal and state laws.

The purpose of this policy is to ensure compliance with the standards set forth by the University to be adhered to by all campus units as well as all individuals who operate or use the computing systems and networks. Violation of these policies is grounds for revocation of system privileges, disciplinary action, and/or criminal prosecution.
- II. Inclusions** - The College of Agricultural & Life Sciences' technology resources includes University-owned computers, peripherals, and related equipment and software; classroom technologies; computing and electronic communication devices and services, including modems; electronic mail; phones; voice mail; facsimile machines, multimedia and hyper media equipment and related supporting devices or technologies.
- III. Incidental Personal Use** - Incidental Personal Use is accepted and appropriate use for CALs employees. It includes non-University related activities such as use of e-mail to send personal messages to friends, family, or colleagues, and use of the Internet for personal use. However, this type of personal use must still adhere to all University appropriate use policies, and must never have an adverse impact on uses of technology and information resources in support of the University's missions. Each department/center reserves the right to determine the level of incidental personal use allowed in their departments/centers. An employee's supervisor may also decide that personal activities are affecting the abilities of the employee or colleagues to perform job functions, and it is their right to ask the employee to cease those activities or risk disciplinary action.

IV. Individual Privileges

Reasonable Confidentiality/ Security - The College of Agricultural & Life Sciences systems provides reasonable security against intrusion and damage to files stored on the central computing facilities. CALS also provides some facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, neither the College or staff can be held accountable for unauthorized access by other users, nor can they guarantee protection against media failure, fire, floods, etc.

Every effort will be made to ensure the privacy of a user's account. In some situations that threaten the network, however, an account may be accessed by the appropriate authority to determine the potential of disruption to the network. If a likely situation were to occur, a reasonable attempt to contact the user will be made before accessing account information. By accepting a user account, the user agrees to this policy.

V. Individual Responsibilities

Courtesy and Respect for Others - You are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.

Harassment - No member of the community may, under any circumstances, use CALS computers or networks to libel, slander, or harass any other person.

The following shall constitute computer harassment: 1.) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's family. 2.) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease. 3.) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease. 4.) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another. 5.) Intentionally using the computer to invade the

privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

Individual Access - Each individual given access to the system will be issued a secure account. It is the individual's responsibility, however, to take precautions to ensure the security of your account. Protect your data and the systems you use. For example, back up your files regularly. Set an appropriate password and change it regularly. Use encryption of data when possible. Make sure you understand the access privileges you have set for your files and computer system. It is against University standards and regulations to give account passwords and other information out to the public. Violating this rule leaves your account and the entire system vulnerable to the public. Persons may not obtain, use, or attempt to obtain or use passwords or network IDs or other network codes that have not been assigned to them as individuals or authorized for their use as University employees. Persons may not obtain or attempt to obtain unauthorized access to computer accounts, software, files, or any other University resources.

Impersonation and Anonymity - You must not claim to be someone else, or claim to have a different relationship to the College than you actually do when obtaining a computer account or access to a lab. You must not falsify your name, address, e-mail address, or affiliation when sending e-mail or other messages from a CALS computer. Doing so may be illegal as well as being an unacceptable use of the College's facilities. On some systems, there are ways to post messages without revealing your name and address. Anonymous communication is permissible when there is a legitimate need for additional privacy. It is not a cover for fraudulent or obnoxious behavior, and in cases of abuse, anonymous messages may be traced to their source. Deceptive communication, in which you claim to be some other specific person, is never permitted.

Copyrighted Information - Written permission from the copyright holder is required to duplicate any copyrighted material. This includes duplication of audiotapes, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose. Most software that resides on CALS computing networks is owned by the College and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses.

Political Campaigning - No user shall use the CALS computers or system to support or gain support for an individual running for public office unless authorized by an appropriate University department.

Personal Business - Authorized users may access CALS computing equipment, systems and networks for personal uses if it does not result in

commercial gain or private profit, except as allowed under policies relating to University intellectual property and external activities for pay. However, in no case may CALS computing resources be used for solicitation of external activity for pay.

Viruses - No one shall create, install, or knowingly distribute a computer virus or other surreptitiously destructive program on any CALS computer or network facility regardless of whether any demonstrable harm results. Use of the computers to circulate chain letters and pyramid schemes is not permitted. If someone asks you to forward a copy of e-mail to "everyone you know" don't. Such messages often contain misunderstood or outdated information, or even outright hoaxes.

VI. College of Agricultural & Life Sciences Computer Privileges

Imposition of Sanctions - CALS reserves the right to impose sanctions and punishments on anyone who violates the policies of the College regarding computer and network usage.

System Administration Access - A system administrator may access others files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

Violations/Penalties - The College of Agricultural & Life Sciences and its authorities are authorized to investigate alleged or apparent violations of College policy or applicable law involving CALS systems using whatever means appropriate. It is also a responsibility of the users of the College's computers and network, to notify the proper authorities if any violation of these policies occurs.

System Administrators are authorized by the College to investigate policy violations and apply temporary reduction or elimination of access privileges while the matter is under review. These temporary sanctions may apply to computing accounts, networks, CALS-administered computing rooms, and other services or facilities.

A user accused of a violation will be notified of the charge and will have an opportunity to respond to the CALS disciplinary body appropriate to the violator's status, before a final determination of any penalty.

When applicable through local, state or federal law, violations may be brought to the attention of police authorities and the College reserves the right to commence legal actions where appropriate.

VII. College of Agricultural & Life Sciences Responsibilities

Security Efforts - CALS has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.

Anti-harassment Efforts - CALS has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and to impose the appropriate penalties when such harassment takes place.

Contact Names - If any questions arise regarding this policy, please contact the Director of Human Resources (2-3337), Administrative Computing Services (2-6108) or the Associate Dean for Administration (2-9812).