

INTRODUCTION

This policy is designed to enhance the quality of the computing environment at Life University ("LIFE" or the "University") and to further the academic, research and public service mission of the University. This requires equitable computer resource distribution, computer and network availability, personal privacy, and data integrity. Achieving these goals requires cooperation and adherence to the following guidelines by LIFE's faculty and staff. This Policy applies to all computer, network and computer communication facilities which LIFE owns, leases, uses, operates or to which LIFE provides access. Use of a Life University computer, system or network acknowledges consent to all of the terms of this Policy.

RIGHTS AND RESPONSIBILITIES

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and it is imperative that all users act in a responsible, ethical and legal manner. This means respecting the rights of other users and the integrity of the systems, and observing all relevant laws, regulations, license agreements and contractual obligations. Users must recognize that the Life University community shares information technology resources, and therefore must not waste those resources, prevent others from utilizing them, harm the University's computer resources and information, or use those resources to harass, abuse or discriminate against others.

PRIVACY AND MONITORING

All users must respect the privacy and usage privileges of other users. LIFE endeavors to respect the privacy of its users, but users should be aware that such privacy is not absolute. LIFE periodically conducts security and performance testing which may temporarily compromise the privacy of information or communications on LIFE's computers or systems. LIFE may also access user files or suspend services without notice to protect the integrity of its computer systems or to investigate possible unauthorized or improper use. LIFE does not exercise editorial control over information stored on its computers or systems and is a carrier of information, not a publisher of information, on its computers or systems. As such, LIFE should not be expected to be aware of, or directly responsible for, material that users send or transmit on LIFE's computers, systems or network.

AUTHORIZED USE

Individuals who have active, authorized accounts on a LIFE computer or network are considered authorized users. Authorized use by those individuals is that which is consistent with the academic, research and public service goals of this institution and comports with the guidelines of this Policy.

EXAMPLES OF MISUSE

Examples of misuse include, but are not limited to, the following:

- Use of LIFE's computer resources by any unauthorized user. In addition, if any authorized user allows another person access to the University's computer resources, the authorized user is held accountable for any actions taken by the individual to whom the authorized user permits access.
- Giving your password to another user for the purpose of sharing your personal account.
- Using LIFE's network or any LIFE computer to gain unauthorized access to any computer system.
- Knowingly interfering with the normal operation of LIFE's computers, systems or networks.

- Using a computer account or obtaining a password that you are not authorized to use. You are responsible for security on accounts and machines provided for your use. This includes setting and changing passwords appropriately to protect their confidentiality.
- Masking the identity of an account or machine. This includes sending mail anonymously or sending mail that appears to come from someone else.
- Knowingly running or installing on any LIFE computer, system or network, or giving to another user, a program intended to damage or place excessive load upon a University computer, system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, worms or password-cracking systems.
- Attempting to circumvent data protection schemes to find security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computer resources.
- Using electronic mail to harass or intimidate others.
- Posting material on electronic bulletin boards or sending electronic mail which violates existing laws of LIFE's Codes of Conduct.
- Attempting to monitor or tamper with another user's electronic communications.
- Reading, copying, changing or deleting another user's files or software without explicit agreement and permission.
- Using your account or access to LIFE's computer resources for any commercial enterprise, personal financial gain or political activity, or for any activity that is commercial in nature, such as advertising, consulting services, typing services or developing software for sale.
- Theft or damage of LIFE's computer equipment, hardware or software.
- Campus-wide electronic mailings without prior permission from a System Administrator (due to the heavy use of resources this requires).
- Unapproved game-play using the University's computers or networks. Policies regarding game playing on LIFE's computers or networks are established by individual departments. No department should permit game playing to interfere with normal business activities.
- Accessing, transmitting, printing, copying or displaying lewd or pornographic material.
- Using a LIFE computer, system or network to send mass mailings or mailings to a mass distribution list without prior permission from both the appropriate Department Head and the Network Coordinator.
- Sending chain letters or information regarding pyramid schemes.
- Failure to respect another's privacy.

SYSTEM PROTECTION AND TESTING

Activities will not be considered misuse when authorized by appropriate Life University officials for security or performance testing. Life University System Administrators may access user files or suspend services without notice in order to protect the integrity of LIFE's computer systems or to investigate possible unauthorized or improper use.

SUSPECTED MISUSE

If you suspect that your computer account has been compromised or other misuse on the system has occurred, you should immediately contact a System Administrator or Network Coordinator.

ENFORCEMENT AND CONSEQUENCES OF MISUSE

Minor infractions of this Policy or those appearing to be accidental in nature may be handled in an informal manner such as electronic mail or in-person discussion. More serious infractions are handled through formal procedures which may include suspension, demotion, dismissal, adjustment of pay to a lower level for a specified period of time, and other actions affecting current pay, merit status or tenure admonition, temporary or permanent suspension of computer, network or computer lab privileges, and referral to appropriate campus committees, including the Academic Review Committee and Student Judiciary Committee. Misuse may also result in federal and state legal prosecution. Illegal reproduction of software protected by United States copyright law may result in civil damages and criminal penalties, including fines and imprisonment. Additional penalties and sanctions are outlined in the Georgia Computer Systems Protection Act, O.C.G.A. 16-9-90 et seq., and the Federal Electronic Communications Privacy Act of 1996.

COMMUNICATIONS WITH SYSTEM ADMINISTRATORS

Life University faculty and staff computer users are expected to read sign-on messages and other posted system news for information concerning system changes, policy changes and scheduled downtime. System Administrators may find it necessary to contact you regarding policy issues. If repeated attempts to contact you are unsuccessful, a System Administrator may be forced to temporarily deactivate your account.

FOR MORE INFORMATION

Questions regarding this Policy can be directed to a System Administrator or to the Director of the Office of Information Technology.