THE LEADER IN GLOBAL EDUCATION

FAIRLEIGH DICKINSON UNIVERSITY

ACCEPTABLE USE POLICY FOR COMPUTER USAGE

Table of Contents

This policy is published by the Office of Information Systems and Technology (IST) and is subject to revision. Comments and suggestions are welcome and should be sent to Brian Domenick, University Director of Information Systems and Technology, mailstop T-BH1-01, or brian@fdu.edu.
This document is updated semi-annually and is available both electronically and in printed form at each of the Campus Computing Centers.
It is the user's responsibility to remain informed about the contents of this document.

Last updated: December 12, 2000

Fairleigh Dickinson University

ACCEPTABLE USE POLICY FOR COMPUTER USAGE

The computing and electronic communications resources at Fairleigh Dickinson University support the instructional, research, and administrative activities of the University. Users of these facilities may have access to University resources, sensitive data, and external networks. Consequently, it is imperative for all users to behave in a responsible, ethical, and legal manner. This document presents specific guidelines to appropriate behavior and use of FDU computing equipment.

I. SCOPE

These guidelines apply to all users of computing and electronic communications resources, and computing equipment owned, leased or rented by Fairleigh Dickinson University. This includes all students, faculty, visiting faculty, staff, guests of the administration, and external individuals or organizations. Computing equipment includes, but is not limited to, the dialup modems, terminals and microcomputers in public labs, minicomputers, file servers, and networking equipment used to link these components together and to the Internet. Fairleigh Dickinson University is not responsible for the content of any material the user prepares, receives or transmits. Thus, as a condition of using the University's computer system, the user represents that he/she is in compliance with all federal, state and international copyright and other intellectual property laws and agreements and other federal and state laws, nor in his/her use of the system will the user violate any federal or state civil or criminal laws. Furthermore, the user will indemnify, exonerate and save the University (and its representatives) harmless from any claim, damage or cost related to the user's use, including any legal fees the University decides it is necessary to incur to defend itself.

II. ACCEPTABLE USE

Those who make use of the FDU computing network are required to behave in a manner consistent with FDU's codes of conduct. As a user of this network, you agree to the following usage guidelines:

1. You are responsible for any computer account you have been given. You shall set a password on the account that is not easily guessed and shall not share this password with other people. If you discover that someone has made unauthorized use of your account, you should change your password immediately and immediately report the event to one of the individuals listed in appendix 1. You also shall not use an account not belonging to you.
2. You agree not to intentionally seek out information about, copy, or modify password files, other users' files, or disks and tapes belonging to other people, whether at FDU or other facilities.
3. You should not attempt to decrypt material to which you are not entitled or attempt to gain rights you have not been specifically granted by the owner. If you observe or discover a gap in system or network security, you agree to inform the Computer Center and not to exploit the gap.
4. You agree to refrain from any activity that interferes with a computer's operating system or its logging and security systems, or that may cause such effects.
5. You must be sensitive to the public nature of computer systems and refrain from transmitting, posting or otherwise displaying material that is threatening, obscene, harassing or defamatory.
6. You agree not to make copies of or distribute software the University owns or uses under license, unless the owner of the software or the owner of the license has specifically granted permission to copy. If in doubt as to whether you have permission to copy software, assume you don't.
7. Messages, statements, and declarations sent as electronic mail or public postings should be treated as if they were tangible documents. From electronic identifiers used in the transmission of messages, addressees can see the University is the source of the message or its system is being used to transmit it, similar to how letterhead or return addresses on a tangible document would identify the University. To make sure that no addressee can infer that your personal opinions are necessarily shared or authorized by the University, it is your obligation to clearly identify them as your opinions and not those of the University.
8. You agree not to create, alter, or delete any electronic information contained in any system associated with the Computer Centers that is not your own work.
9. You agree not to create & send, or forward electronic chain mail letters. You agree not to attempt to alter or forge the "From" line or any other attribution of origin contained in electronic mail or postings. You agree not to use any of the university systems for sending what is commonly referred to as "SPAM" mail (unsolicited bulk email).
10. You shall not use FDU computing equipment as a means of obtaining unauthorized access to any other computing systems.
11. FDU's computing disk storage is a University resource with costs attached and should be used with care and discretion. It is not meant to be used for archiving programs and data not currently being used or for storage of

files publicly available elsewhere. It is meant for current class work, research and development projects, and temporary storage of other files. Users shall attempt to keep their disk usage minimized and will refrain from maintaining duplicate copies of software already installed on the system.

12. Network addresses such as TCP/IP addresses and machine addresses are assigned by University Systems and Security staff and may not be altered or otherwise assigned without the explicit permission of the University Director of Information Systems and Technology. In addition, no equipment may be attached to the network without the explicit permission of the University Director of Information Systems and Technology.
13. The system is not to be used for the transmission of commercial or personal advertisements, solicitations, and promotions or for extended reproduction of political, ideological or commercial material originated by a person or organization. This includes but is not limited to the execution of revenue-generating advertising programs, which pay users when the programs are run. The University Director of Information Systems and Technology may suspend this rule when it is in FDU's best interest to permit such activity.
14. In the quantity and frequency of their personal use, users should not create unreasonable demands on the system. Users are reminded that for volume or frequency beyond what is reasonable for their free access to the University's network and systems, they should contract with private providers of network facilities.
15. Without the explicit permission of the University Director of Information Systems and Technology you agree not to run any of the following protocols or services:

    A. Port scanners, network monitors or other types of utilities on any part of the university's network.

    B. Routing or network serving protocols such as RIP, IGRP, BOOTP or DHCP on the network.

    C. Daemons, processes or programs that accept incoming connections as a server would.

16. FDU's computing network, services, and wiring may not be modified or extended beyond the areas of their intended use.
17. Network connections may not be used to provide network access to anyone outside the University community or for any purposes other than those that are in direct support of the academic mission of the University.
18. Department Heads and other administrators may enact additional restrictions to these policies to further limit usage by employees. These restrictions may include but are not limited to: limiting time spent reading or writing personal email or visiting web pages, and limitations on

acceptable content due to the possible exposure of screens to other individuals.

III. SECURITY

Users should use any available methods to safeguard their data, including regular changes of passwords, making duplicates of files, and encrypting sensitive data. In the event that files have been corrupted as a result of intrusion, you should notify a system administrator immediately. Please note that the computer systems are not completely secure. It is possible that others will be able to access files by exploiting shortcomings in system security. For this and other reasons, FDU cannot assure confidentiality of files and other transmissions.

Information Systems and Technology and each of its departments attempt to provide reasonable security against damage to files stored on FDU's computing equipment by making regular backups of systems. In the event of lost or damaged files, a reasonable attempt will be made to recover the information; however, the University and the Computer Center staff cannot guarantee recovery of the data or loss of data due to media failure, floods, fires, etc.

Information Systems and Technology and each of its departments will make reasonable attempts to provide error-free hardware and software on our systems, however, it is not possible to guarantee this, and information provided by staff members is not guaranteed to be correct.

IV. PRIVACY

Users should exercise caution when storing any confidential information in electronic format, because the privacy of such information cannot be guaranteed. Even though the electronic data grams transmitted by or stored on university equipment are the property of the University, the IST staff will not normally log into another user account or access user's files unless specifically granted permission by the owner of the file. Student staff should avoid situations where helping another student or a faculty member would give them access to data relevant to a course that the student staff person is currently taking.

Exceptions to this practice are made under certain circumstances. These include: system backups, which access all files in a user's account; software upgrades which may require editing startup files in a user's account; diagnostic and trouble-shooting activities, which may, for example, require viewing the address headers of e-mail messages to determine the cause of problems; and keystroke monitoring of sessions to determine inappropriate use of the computing facilities. Another situation is a suspected violation of the tenets in this policy, the Student Handbook, Faculty Handbook, University employment rules and practices or local, state or federal law. If there is sufficient cause to suspect such a situation, a user's files may be duplicated and stored for later review by appropriate personnel without the user's permission. Users of FDU systems are hereby informed that they have no justified expectation of privacy in material processed, sent, or stored on or through the systems, and that the consent of the user to give access to his or her electronic documents is a condition precedent to the user's use of the system. In the event that user files need to be copied or viewed for reasons other than security, diagnostic, system backup or in compliance with law enforcement, Information Systems and Security staff will attempt to inform the user of this access.

The Family Education Rights and Privacy Act (FERPA) bind all users who have access to student data. Its application relevant to this Acceptable Use Policy centers on a student's right to consent to disclosure of personally identifiable information. FERPA does permit certain information to be released without consent and this information is referred to as Directory information. To find out specifically what information you may or may not give out and to whom, you may contact the Dean of Students office. There is also information on FERPA in the Student Handbook. When you are in doubt as to whether or not you are permitted to release some information, do not release the information until you know for sure.

V. POLICY VIOLATIONS

Policy violations should be reported immediately to any one of the individuals listed in Appendix 1.

Depending on the nature of the events, violations of this policy may be dealt with as described in the Student or Faculty Handbook, any relevant contracts, and possibly State and/or Federal law or regulations. In addition, a user's system privileges can be suspended for a specified time period or revoked as decided by the appropriate Provost or Division Vice President and a monetary fine on those in violation may be levied to reimburse the University for the staff time and other costs of investigating and rectifying the violation. The person on whom a sanction or fine is imposed can appeal to the Executive Vice President in writing within 10 days.

University Systems and Security reserves the right to suspend network and/or system privileges while investigating a complaint or troubleshooting a system or network problem.

Appendix

Computer Center Contacts

Neal Sturm
Associate Vice-President
Information Resources and Technology
Mailstop M140B
973-443-8689
sturm@fdu.edu

Brian Domenick
University Director for Information Systems and Technology
Mailstop T-BH1-01
201-692-2414
brian@fdu.edu

Saul Kleinman
University Director of MIS
Mailstop T-BH2-03
201-692-2065
saul@fdu.edu

Melanie Scarpa
Director of Telephone & Voice Services
201-692-7390
scarpa@fdu.edu

Ralph Knapp
Director, Computing Services (Florham-Madison)
Mailstop M140B
973-443-8689
knapp@fdu.edu

Robert Pelech
Director of Computing Services(T-H)
201-692-7111
bob@fdu.edu