

Computing Access Agreement

Introduction

The College of New Jersey computer systems and network are provided to support the mission of the College. Students, faculty and staff are encouraged to use computing facilities to enlarge their potential for making solid contributions to our society. As a provider of network and computing services to the campus, the College has an obligation to establish regulations for their use in order to benefit the entire community. Computer users do not own accounts on College computers, but are granted the **privilege** of exclusive use of an account. While the College does not monitor transmissions for the purpose of censorship, in order to promote and protect acceptable ethical, moral and legal standards, the college may monitor transmissions should a violation of these regulations be alleged. Failure to comply with acceptable standards may result in a suspension or revocation of privileges.

Eligibility of Computing Accounts and Network Access

Students, staff and faculty of the College may use the Information Technology computer systems and connected networks to which they have been granted access for purposes of research, education or College administration. To be eligible for a computing account, students must be enrolled for a minimum of one course. A lapse in enrollment could result in the loss of computing privileges during that period of non-enrollment. Accounts are available to full and part time faculty and staff during their employment at the College. College departments may request that adjunct faculty accounts remain for up to one year to alleviate the deletion and recreation of accounts for adjunct faculty who regularly teach only one semester a year.

Access to the College network is ultimately granted by Information Technology. Faculty and staff must be granted permission from their department before Information Technology will connect their office or computing device to the network. **No device may be connected to the College network without the knowledge and authorization of Information Technology.**

Privacy of Computer and Network User Information

Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), users are entitled to privacy regarding information contained on their accounts. In addition, certain student records on College computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section 1232[g]). **However, it should be noted that there are no facilities provided by the College systems for sending and receiving confidential messages and files.** Also, the Electronic Communications Privacy Act of 1986 allows system administrators or other College employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the College. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.

Software Use Guidelines

The College has subscribed to the following statement on software and intellectual rights distributed by EDUCOM, a non-profit consortium of over 592 colleges and universities committed to the use and management of information technology in higher education, and by ADAPSO, the computer software and services industry association: "Respect for intellectual labor and creativity is vital to academic discourse and intellectual enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution." "Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

Unacceptable Conduct

All existing policies and regulations of The College which govern student and faculty conduct, including but not limited to the Student Handbook, are hereby incorporated in this Computer Access Agreement and shall govern the conduct of students and faculty who utilize The College's network and computing services.

Following is a list of unacceptable conduct on the College computer accounts, College computer systems and the College network. This list includes, but is not limited to:

- Use of College computer systems or College computer accounts to resell Internet service.
- Use of College computer systems or College computer accounts for commercial use that results in technical difficulties. If difficulties result, Information Technology will notify the account holder immediately.
- Use of computer accounts, computer systems or the network to violate any state or federal laws.
- Use of computer accounts, computer systems or the network to harass or violate the rights of others.
- Use of computer accounts, computer systems or the network to gain access or use resources for which one does not have authorization.
- Use of the network to disrupt the work of the others either locally or on the Internet. Examples of activities that may be disruptive include, but are not limited to, games, broadcast e-mail, "chainletter" e-mail, excessive use of network "chat" programs.
- Modifying or extending network services and network wiring without prior written consent from the College.
- Use of computer accounts, computer systems or network connections to provide access to anyone outside of the College community for any purpose other than those that are in direct support of the academic mission of the College.
- Forging the identity of a user or a machine in an electronic communication. Prosecution under state and federal laws may apply.
- Use of College owned computer facilities by non-College members.
- Unauthorized attempts to circumvent data protection schemes or uncover security flaws. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Use of a computer account that was not assigned to you by Information Technology, unless multiple access has been authorized for the account and the owner of the account has explicitly given you access.
- Use of College computing resources by College employees for personal use without the approval of the department in which the resource is located.
- Use of computer accounts, computer systems or the network to violate any College rule.

Enforcement

It is essential for each user of the network to recognize the responsibilities that accompany the privilege of having access to a vast array of resources. Users are ultimately responsible for their own actions in accessing network services. **The use of the network is a privilege which can be revoked at any time for abusive conduct. Violators are subject to criminal prosecution and/or disciplinary action through the College judicial structure or personnel hearing process.**

Information Technology, Human Resources, Campus Police and Student Life enforce these policies as they relate to their areas of responsibility. Campus Police may involve other law enforcement agencies as necessary. In addition, the College department in which the violator is employed may be involved. Harassment or threats should be reported to Campus Police immediately. Other issues involving student violations of these guidelines should be reported to the Vice President of Student Life office. Any remaining issue should be directed to Information Technology and the Office of Human Resources. **The College reserves the right to disable a computer account to preserve evidence under investigation. The College also reserves the right to view files in user accounts, on backup tapes or in transit on the network as is necessary to complete an investigation.**

User Responsibilities

- Computer system users are advised that it may be unwise to store confidential files or receive confidential messages on College computer systems.
- If you create or maintain electronically-stored information which is important to your work or to the College in general, you are ultimately responsible for making frequent backups of the information. Information Technology makes a reasonable attempt to ensure the data and software on multi-user College computer systems are backed up regularly.
- Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings or provided as electronic documents (web pages for example) must meet the same standards for distribution or display as if they were tangible documents. They should be identified as coming from you, or, if you are acting as the authorized agent of a group recognized by the College, as coming from the group you are authorized to represent. Attempts to alter the "From" line or other attribution of origin of electronic mail, messages, or postings, will be considered transgressions of College rules.
- Adherence to the "Policy Regarding Public Presentations on the Internet/WWW" (this document is available separately).
- Computer system users must make a reasonable attempt to protect their account from being accessed by others. This includes having a secure password and maintaining proper access permissions on sensitive files you may have in your account. Passwords are encrypted in the system and must be reset. If you need your password reset, you will need to come to the Help Desk to have any action taken on your password. You should never keep a session open when you leave your terminal.
- All electronic mail files belong to somebody. They should be assumed to be confidential, unless the owner has explicitly made them available to others.

Disclaimer

- The College assumes no responsibility for the accuracy of information obtained from sources outside the control of the College. This includes, but is not limited to areas such as the Internet, unofficial web pages, personal web pages and personal e-mail.
- No computer system can absolutely prevent determined persons from accessing stored information they are not authorized to access. The College, therefore, cannot guarantee the privacy of electronic documents.
- **The College assumes no responsibility for the loss of data on an individual's microcomputer due to computer viruses, other willfully destructive software or as a result of flaws in the application or operating software on the microcomputer.**

This document is subject to change without notice. It is your responsibility to periodically review this document for changes and comply with them.

Last Updated: December 14, 2000 (changed Information Management to Information Technology)

Copyright © 1996-2000 The College of New Jersey

Portions copyright © 1994 Drexel University, © 1995-1996 Princeton University, © 1993-1995 Regents of the University of California. Used with permission.