

# IT Acceptable Use Policies

Chatham University Computing Policies  
**Information Technology**  
**August 1999**  
**Revised March 2008**

Based on the Computing Policies of Wake Forest University -- Winston-Salem, NC  
**Computing Usage Policies and Procedures**

This policy is intended to promote the responsible and ethical use of the computing resources of Chatham University. In light of the contribution that computers can make to furthering the educational and other objectives of the University, it is in the best interest of the community as a whole that computing resources be used in accordance with practices which ensure that the rights of all users are protected and the goals of the University are achieved. The following policy applies to all students, faculty, and staff who use the Chatham University Computing Network.

## General Information

- The Chatham University Computing Network is for use by the students, faculty, and staff of Chatham University for the furthering of the instructional and operational objectives of the University. The same ethical standards which apply to other University activities apply to use of the Chatham University Computing Network including the Chatham University Honor Code, and all local, state, and federal laws. Use of the Chatham University Computing Network is restricted to authorized users. For the purposes of this document, an "authorized user" is defined as an individual who has been assigned a login ID and password by the Information Technology staff, or by an authorized agent. Individual users are responsible for the proper use of their accounts, including the protection of their login IDs and passwords. Users are also responsible for reporting any activities they believe are in violation of this policy, just as students are responsible for reporting Honor Code violations.
- Student User Accounts/Email Accounts are retained for one full semester after graduation. The Accounts will be deleted after this time period.
- Staff User Accounts/Email Accounts are disabled/deleted upon termination. Any extension to this policy must have prior approval from the Director of Human Resources.
- This policy applies to all computer and computer communication facilities owned, leased, operated, or contracted by Chatham University. This includes word processing equipment, microcomputers, minicomputers, mainframes and associated peripherals and software, regardless of whether used for administration, research, teaching, or other purposes. This policy also extends to any University facilities used to access computer facilities elsewhere.

## Changes to This Policy

- This policy is provided to all users of the Chatham University Computing Network, and every effort is made to ensure that all users will view the policy at least once. Information Technology may change or amend this policy at any time. When changes are made, they will be announced. Users shall observe any new policies immediately after the announcement is posted, or as directed.

## Basic Principles

- As in all aspects of University life, computing facilities users should act honorably and in a manner consistent with ordinary ethical obligations. Cheating, stealing, making false or deceiving statements, plagiarism, vandalism, and harassment are just as wrong when done in the context of computing as they are in all other aspects of University conduct.

Individuals should use only those computing facilities they have been authorized to use through ordinary channels. They should use these facilities:

- In a manner consistent with the terms under which they were granted access to them
  - In a way that respects the rights and privacy of other users
  - So as not to interfere with or violate the normal, appropriate use of these facilities
  - In a responsible and efficient manner
- Chatham University computing resources are not to be used for commercial purposes or non-University related activities without prior written permission. Individuals should respect the rights and privacy of other authorized users. Thus they should respect the rights of other users to security of files, confidentiality of data, and the ownership of their own work. Users should refrain from:
    - Using the computer access privileges of others Accessing, copying, or modifying the files of others without their explicit permission
    - Illegal copying of software or data
    - Harassing others in any way or interfering with their legitimate use
  - Individuals should not attempt to interfere with the normal operation of computing systems or attempt to subvert the restrictions associated with such facilities. They should obey the regulations affecting the use of any computing facility they use.

## **Elaboration**

The purpose of the following list is to aid in interpreting the principles listed above. This list should in no way be construed as comprehensive. Examples of actions in violation of these principles include:

- To turn in a paper or computer program as his/her work that was created by another individual Copying of licensed or Copyrighted software not permitted by law or by contract
- E-mail messages containing material of an obscene nature, or material of a harassing nature, are expressly forbidden. The sending of "chainletters" or "email spamming" is also forbidden. Anyone receiving any such material should forward the entire message to 'postmaster@chatham.edu.
- Sending electronic mail fraudulently, for example, by misrepresenting the identity of the sender
- Utilizing a loophole in a computer's operating system or knowledge of a privileged password to damage a computer system or to gain access to a system or resource which one is not authorized to use
- Using University computing facilities for commercial purposes, without written approval by the Assistant Vice President for Information Services
- Knowingly allowing another person to use the account privileges for improper purposes
- Turning in someone else's paper or computer program as personal work
- Reading someone else's electronic mail without his/her permission Using University facilities to gain unauthorized access to computer facilities off-campus
- Intentionally using an abnormally large amount of resources, such as processing time or disk space, without prior permission from the I.T. Department
- Installing personal software on University owned computers unless express permission from the I.T. Department is granted
- Tampering with University owned computers in any way that would degrade the system
- Circumventing virus protection programs or knowingly distributing virus infected files using the Chatham University Computing Network

## Privacy

- In order to enforce the policies herein, Information Technology staff is permitted to monitor all activity on the Chatham University Computing Network. The staff must strive to protect the privacy of users. In general, staff may search the file system for potential violations as specified in the section on System Monitoring below, and when there is evidence of a possible violation, they may view user's files, read mail, monitor keystrokes, and otherwise observe users activities, in accordance with the Computer Usage Policy.
- In the event that staff should investigate a user, a record of the investigation will be placed in a permanent file to be kept in Information Technology. All user investigations must be approved by the Director of Information Technology. This record shall state why the user was investigated, what files were examined, and the results of the investigation. Information Technology staff will not reveal the contents of users' files, users' activities, or the record of investigations except under the following circumstances, and only with the approval of the Director of Information Technology and/or the Director of Human Resources and/or the Vice President of Student Affairs .
  1. Evidence of Honor Code violations will be referred to the Vice President of Student Affairs.
  2. Evidence of improper activities by employees will be referred to the Director of Information Technology or the appropriate University officers
  3. Evidence of violations of law will be referred to the appropriate law enforcement officials
- Should Information Technology receive an inquiry concerning whether a user's access is suspended, Information Technology staff will provide only a confirmation and the dates on which access is to be denied and restored. No information regarding the reasons for suspension will be provided to anyone except the user and the authorities noted above.

## System Monitoring

- This policy statement serves as notice to all users of the Chatham University Computing Network that regular monitoring of system activities occurs. Staff routinely monitors the following information:
  1. System log files, which contain information pertaining to all processes executed on the system, are examined.
  2. System directories, temporary storage areas, work areas, and all areas outside of users' home directories and mail files are examined.
  3. Mail messages with invalid recipient or sender fields are frequently sent to the Postmaster who examines them to determine the cause of the problem.
  4. Unsuccessful attempts to log into an account will be monitored.
  5. Attempts to disguise the source of electronic mail will be monitored.
  6. Any activity which, in the opinion of the staff, appears to compromise the security or integrity of the operating system is monitored.
  7. A complaint brought by another user will result in examination of relevant information.
- Only the following persons are authorized to engage in such monitoring: the Director of Information Technology, Manager of Administrative Computing, Manager of Internet Services, and the Systems and Networks staff.

## Prohibited Activities

- The following activities are prohibited on the Chatham University Computing Network, in addition to activities prohibited by the Computer Usage Policy of Chatham University
  1. Providing any unauthorized user with access to a personal login ID, or in any way allowing others to access the machine, is prohibited. This includes providing access to resources on the Chatham University Computing Network without the express written permission of Information Technology. For example, two authorized users of the Chatham University computing network may share access to each other's login IDs, but they may not give their login IDs to anyone who does not already have an authorized login ID on the Chatham University computing network.
  2. Intentionally creating, modifying, or copying files to or from any areas to which the user has not been granted access, is prohibited.
  3. Disguising one's identity in any way, including the sending of falsified messages, removal of data from system files, and the masking of process names, is prohibited.
  4. The establishment of any function, which provides unauthorized access, via the Internet connection or otherwise, without the written permission of Information Technology is prohibited. For example, users may not install games, which allow users to access the Chatham University Computing Network without a valid login ID.
  5. Any use not consistent with instructional and research purposes, such as commercial activity, is prohibited.

## Disciplinary Actions

- Reasonable suspicion of a violation of the principles or practices described in this policy statement may result in disciplinary action. Such action will be taken through appropriate University channels such as administrative procedures, the Judicial Board, or other supervisory authority to which the individual is subject. Violation of State or Federal statutes may result in civil or criminal proceedings.
- Nothing in this statement diminishes the authority and responsibility of Information Technology to take remedial action in the case of possible abuse of computing privileges. To this end, Information Technology, with due regard for the right of privacy of users and the confidentiality of their data, have the right to suspend or modify computer access privileges, examine files, passwords, accounting information, printouts, tapes, and any other material that may aid in maintaining the integrity and efficient operation of the system. Users whose activity is viewed as a threat to the operation of a computing system, who abuse the rights of other users, or who refuse to cease improper behavior may have their use privileges revoked.
- Violation of the Computer Usage Policy or any of the policies herein will result in the immediate suspension of the user's access. Upon suspending a user's access, Information Technology will notify the user in writing within 24 hours. The notice will clearly state which policies were allegedly violated. The suspended user must contact the Assistant Director of Information Technology regarding the suspension. After discussing the alleged violation, the Assistant Director of Information Technology in consultation with the Director of Information Technology may restore the user's account, or suspend the user's account for up to one year. If the user has not contacted the Assistant Director of Information Technology within seven days of the suspension, the Assistant Director of Information Technology in consultation with the Director of Information Technology will render a decision on the suspension and notify the user as specified below.
- In the event that a suspended user and the Assistant Director of Information Technology and the Director of Information Technology are unable to resolve the matter to the user's satisfaction, he or she may appeal to the Vice President for Finance and Administration

within seven days. The Vice President for Finance and Administration may reactivate the user's account, reduce the length of the suspension, or uphold the decision. When a user's access is suspended, a written notice is sent to the user explaining the length of the suspension and the violations, which occurred. Copies of this notice will be sent to the Vice President of Academic Affairs, Vice President for Finance and Administration, and Vice President for Student Affairs (when a student is involved). Information Technology will also forward this notice to the authorities specified above if there is reason to believe a violation of other University policies or law has occurred.

### **Software Duplication and Use Policy**

- Chatham University licenses the use of its computer software from a variety of companies. The University does not own that software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it. Unauthorized duplication or use of software violates the U. S. Copyright Law and exposes the individuals involved and the University to possible civil and criminal liability. While licensing agreements differ slightly from one software company to another, the license fee generally entitles the licensee to use one copy of the software on one computer. It is usually legal to make a working copy to use with a floppy disk system or to copy onto the hard disk. The original may be kept in a safe place as a backup, and it is usually legal to have a copy of the program included with the system backup. Unless specifically authorized by the license agreement, it is not legal to have copies of the software running simultaneously on multiple machines or to use a single copy on a local area network.
- The best policy for students, faculty, and staff to follow is that copying software for use on additional machines is prohibited unless told otherwise by an authorized individual. The University does not require, request, or condone unauthorized copying or use of computer software and such action is considered not to be taken in the course of employment. As a result, the University cannot provide legal defense for individuals accused of making unauthorized copies of software. If the University is sued or fined because of unauthorized copying or use by students, faculty, or staff, it will be required to seek payment from the individuals. They may also be subject to disciplinary action that may include dismissal. University policy requires that all students, faculty, and staff abide by the law and University contractual obligations.

### **Contacting Information Technology**

To report problems or policy violations, contact the Director of Information Technology at (412) 365-1112.