The College of New Jersey

Section:	tbd
Title:	Client Computing Usage Policy
Effective Date:	1996
Approved By:	
Responsible Unit:	Information Technology
History:	Original document created 1996.
Related Documents:	

INTRODUCTION

The purpose of this policy is to establish appropriate use of client accounts and the College’s computing equipment. The College of New Jersey computer systems and network are provided to support the mission of the College. As a provider of network and computing services to the campus, the College has an obligation to establish regulations for its use in order to benefit the entire community. Computer clients do not own accounts on College computers, but are granted the privilege of exclusive use of an account. At all times, clients using the College’s network and accounts must adhere to legal standards and the ethical and moral standards of the College. Failure to comply with acceptable standards may result in a suspension or revocation of privileges.

DEFINITIONS

For the purposes of this document, the following definitions will apply:

Access - includes wired, wireless, VPN, dial-up, or mobile electronic connection methods [for the purposes of accessing resources] on or off campus.

Account – includes accounts issued via the HR or Student system, or any account issued for access to a third party system

Client – An individual who interacts with a computer to perform processes that yield results, commonly referred to as “client” or “end user”. This includes faculty, staff, students, TCNJ affiliates and authorized guests of the College

Malware – Short for malicious software. Common examples include viruses, worms, Trojan horses, spyware, adware or rootkits. Category of applications that operate usually invisibly on a computer without informed client consent, to:

- gather, modify, or destroy information
- purposefully cause a denial of access to services
- permit unauthorized clients to access the computer or network
- send unsolicited email
- perform other hostile, intrusive, or annoying functions
- or any combination of the preceding

Network access – Access to electronic resources hosted or provided by TCNJ or using TCNJ resources as a transport for access to other networks.

Network Access Device: Device used to connect a computer to a network. Common types include wireless access points and wired switches or hubs.

Status – may include active, inactive and emerti

POLICY

Eligibility for Accounts and Network Access

Clients may use the College computer systems and networks to which they have been granted access for purposes of research, education or College administration. Accounts and access are granted based on each individual’s status and role at the College.

Privacy of Computer and Network Client Information

Information Technology will do its due diligence in taking every precaution possible to protect and secure data. Data security is a partnership between the client and Information Technology. The same security standards that apply to paper files should be applied to electronic files. Each client is responsible for maintaining a level of confidentiality in accordance with their role at the College. **It should be noted that there are no facilities provided by the College systems for sending and receiving confidential messages and/or files and there should be no expectation of data privacy when using the College’s network.**

The College does not monitor transmissions for the purpose of censorship, but may monitor transmissions should a violation of these regulations be alleged. Authorized personnel within Information Technology may also monitor transmissions in the course of performing routine maintenance or troubleshooting network or account problems.

System administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. Client 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. Information Technology professional staff may access college-owned computers to perform system maintenance either on-site or using remote tools as necessary without prior notification.

Unacceptable Conduct

All existing policies and regulations of The College which govern student, faculty and staff conduct, including but not limited to the Student and Employee Handbooks, are hereby incorporated into this Client Computing Usage Policy and shall govern the conduct of students, faculty and staff who use The College's network and computing services. Following is a list of **unacceptable conduct**. This list includes, but is not limited to:

Compliance:

- illegal use or misconduct of any kind (including, but not limited to copyright infringement)
- violation of local, state or federal laws or violation of any College rule or policy
- harassment or violation of the rights of others
- using peer-to-peer (p2p) file sharing unless specific instances are authorized by the College

Network and Internet Access:

- connecting unauthorized devices to the campus network. **No network access device, including but not limited to wireless access points, switches, routers, hubs, network based storage, pico cell technology or personal DHCP servers, may be connected to the College network without authorization from Information Technology.**
- modifying or extending network services and network wiring without prior written consent from the College
- reselling Internet service
- unauthorized access
- using unauthorized resources
- use that disrupts the work of others either locally or on the Internet including initiating "spam" email or use that results in technical difficulties. In either case, Information Technology will take all steps necessary to protect the network.
- using TCNJ resources to send mass emails without administrative approval will be considered "spam" and will be considered a violation of this policy
- masquerading your identity, impersonating other community members, or misrepresenting the College via email, instant message, or other Internet presence will be considered a violation of this policy.
- installing software that may compromise the security of college owned equipment

Data Protection/Privacy:

- providing access to anyone outside of the College community for any purpose other than those that are in direct support of the mission of the College
- forging the identity of a client or a machine in an electronic communication. Prosecution under state and federal laws may apply
- use of College owned computer facilities by unauthorized personnel
- 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 client's electronic communications, or reading, copying, changing, or deleting another client'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/or the owner of the account has explicitly given you access.

Enforcement

It is essential for each client of the network to recognize the responsibilities that accompany the privilege of having access to a vast array of resources. Clients 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 without prior notice. Violators are subject to criminal prosecution and/or disciplinary action through the College student conduct structure or personnel hearing process.**

Information Technology, Human Resources, Campus Police and Student Affairs 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 Affairs office. Any remaining issue should be directed to Information Technology and Human Resources. **The College reserves the right to disable a computer account to preserve evidence under investigation without prior notice. The College also reserves the right to view files in client accounts, on backup tapes or in transit on the network as is necessary to complete an investigation.**

Client Responsibilities

Compliance:

- Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular use. Violation of any federal, state or local law or any college policy will result in account suspension. These include but are not limited to copyright violation, illegal file sharing via peer-to-peer (P2P) networks, software piracy, or violations of FERPA, HEOA or DMCA.

- Adherence to the College's Web Policy found at http://www.tcnj.edu/~academic/policy/webpolicy.html
- When using a personal computer on the College's network, either on campus or remotely via Virtual Private Network (VPN), individuals must comply with the standards set for college computers. Information Technology assumes no responsibility for supporting personal computers on the College's network.

Data Protection/Privacy:

- 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 College servers are backed up regularly.
- When using a shared or open machine such as a computer lab machine, a department machine or a kiosk any data stored to the local hard drive will be lost and unrecoverable when you log off. It is your responsibility to store your data appropriately, either on a network drive or on removable media.
- 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.
- Clients 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.
- It is your responsibility to use strong passwords and to change those passwords often. Do not share your password with anyone. Passwords should not be written down or displayed publicly. Choose a good password at least 8 characters long consisting of uppercase and lowercase letters, numbers, symbols. An abbreviated phrase or sentence with substituted numbers and symbols is a good idea. Information Technology will never ask for your password via email or a web form and by providing such information in either of these formats, the client may put the College's data resources at risk.
- The College is not responsible for personal data stored on college-owned equipment including but not limited to photos, movies, music and personally installed software. Any scholarly work should be identified prior to computer upgrades or maintenance to insure that the appropriate data is transferred.
- Practice good digital citizenship. For more information, refer to http://www.tcnj.edu/~it/security/

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.
- **The College assumes no responsibility for the loss of data on an individual's workstation due to computer malware, other willfully destructive software or as a result of flaws in the application or operating software on the workstation.**