INFORMATION TECHNOLOGY POLICIES and GUIDELINES
For Faculty, Staff and Administrators

Suffolk County Community College makes certain computing resources available to its administrators, faculty and staff to support the instructional, research, student services, public service and administrative activities of the College. These computing resources may include, but are not limited to, host computer systems, communication networks, Internet access, personal computers and peripherals, e-mail, software and data files. None of these facilities are provided for sending or receiving private or confidential electronic information.

Resources are granted to individuals while they are affiliated with the College and, to a limited extent, following retirement and to those designated as *Professor Emeritus*. Those on the adjunct seniority list will continue to have privileges for one year following the last paid assignment. Continuing education instructors will be provided with an e-mail account upon recommendation of the administrator for the area for the period of need. Faculty and administrators are provided access for academic and professional use. Staff are provided access to support their job functions. Incidental personal use is a privilege that will be tolerated as long as it is not abused and conforms to all College policies. It must never have an adverse impact on resources or job performance. Supervisors always retain the right to require that all such personal use cease.

All users of computing resources are presumed to have read, understood and agreed to abide by the Information Technology Policies and Guidelines.

Users of the College's computing resources are obligated to do the following:

1. Comply with the utilization policies of the College's network provider, which presently is SUNYNet/NYSERNET.
2. Maintain appropriate system security, including the protection of personal passwords, so that computing resources are not subject to unauthorized use. Users may not grant permission to others to use their accounts without prior approval.
3. Respect the rights of others to privacy, freedom from theft, harassment, or copyright infringement by not engaging in the following:
    - Unauthorized copying, modifying, or destroying of work on the computer systems, both at the College and available over the network, and from accessing or attempting to access password protected or explicitly restricted computing resources for which the user is not authorized; or
    - Practices which would create a hostile working or learning environment or cause harm to others and/or the system as a whole, including engaging in or disseminating illegal, obscene, threatening, or unwelcome electronic communication, displaying or printing sexually explicit material in a public location, damaging computer resources electronically or physically, or

engaging in conduct that discriminates on a legally prohibited basis. See also the College policies prohibiting discrimination and sexual harassment.

4. Report security violations, including theft, vandalism, or unauthorized access, to the appropriate office.
5. Anyone hosting a web site must include a method for the host to be contacted, and anyone using e-mail services must include a correct return address.
6. Share resources equitably by avoiding activities that place a burden on system resources.
7. Retain e-mail and electronic documents in accordance with New York State laws regulating access to governmental records. Examples of records subject to the law are: policies and directives, correspondence or memoranda related to official business, work schedules and assignments, agendas and minutes of meetings, drafts of documents that are circulated for comment, any document that initiates, authorizes or completes a business transaction, and final reports or recommendations. Such records must be retained for the same periods as paper records of the same nature, and must be stored in a manner that allows for accessibility. These records are subject to the Freedom of Information Law (FOIL) and court subpoena. Those records that contain personal information protected by the Personal Privacy Protection Law (PPPL) must be retained to avoid unauthorized release.
8. Records should be backed up routinely to avoid loss or destruction.
9. Each user is responsible for taking all reasonable precautions to ensure that viruses are not introduced into the College network. Individuals are to follow College procedures and directives to keep virus prevention software current. All material received on a floppy disk or other electronic or optical medium and all material downloaded from the internet or from a non-College computer must be scanned for viruses before being placed onto the College computer system.

Users of the College's computing resources are prohibited from doing the following:

1. Maintaining or operating a non-College enterprise for personal financial gain. (Note: this does not prohibit professional activities in one's College discipline that may incidentally result in personal income, if no staff support or specialized equipment is provided, and if approved by a supervisor as being primarily a professional development activity.)
2. Taking or soliciting orders on an on-going or routine basis or advertising personal services or carrying out the business activities of a not-for-profit entity.
3. Using, decrypting or duplicating software, text, graphics, photographs, recordings, or any other tangible form of expression that would violate or infringe any copyright or similar legally recognized protection of intellectual property rights.
4. Loading or saving software that is not intended for a College purpose, e.g. Subscriber Services (AOL, Prodigy, CompuServe, MSN).
5. Using computing resources for partisan political activities or in any way promoting the candidacy of any person for public office.
6. Sending or forwarding an e-mail from or to a sunysuffolk.edu address that requests the recipient to forward the message to others (e.g. chain letter) when such message is not work-related.

7. Unauthorized attempts to monitor another user's password, password-protected data or electronic communication, or delete another user's data or electronic communication, without that person's permission.
8. Using computing resources to engage in religious activity, except as may constitute incidental personal use.
9. Engaging in bandwidth intensive activities unless approved and scheduled in advance with the Office of Networks and Telecommunications. The following services are blocked on the administrative network unless justified on the basis of College business, and are prohibited on the academic network unless used for professional activities:

   NetRadio, NetTV; Instant Messenger; "PUSH" Servers (AOL, MSN, PointCast); Distributed Shares (Napster, Gnutella); IP Phone
10. Hosting a website or listserv that bears no significant relationship to the duties or professional activities of the user.
11. Possessing, installing, distributing or running on any system connected or with access to the College networks a program that is intended to gain unauthorized access, or is intended to or is likely to result in eventual damage to a file or computer system.
12. Engaging in any intentional, knowing or reckless act that results in denial of service, or damage or destruction to College equipment, property or facilities, or that utilizes College equipment, property or facilities to cause damage or destruction to the equipment, property or facilities of others.
13. Using computing resources in such a way as to hide the identity of the user or pose as another person.
14. Disclosing or disseminating College confidential records to any unauthorized person.
15. Possessing or running any of the following protocols or services on devices connected or with access to the College networks, unless needed to support an academic course the faculty member is teaching at the College: port scanners, network monitors or other types of utilities, routing or network serving protocols, or daemons, processes or programs that accept incoming connection. Where needed to support a course, the individual is required to identify these services and the device to their campus ETU and the Office of Computer and Information Systems.

<u>Privacy Policy</u>

To the extent possible in the electronic environment and in a public setting, a user's privacy will be honored. However, it should be understood that material on the College server or on College desktop equipment is College property (except as may be owned by another in accordance with intellectual property rights). Material may be subject to subpoena or an application to review records under the Freedom of Information Law (as indicated above), and it may be taken by the college (see below) or locked from user access. Also note, this material is not totally secure from unauthorized viewing or editing. While the College will make every effort within its resources to prevent unauthorized access, it cannot guarantee the result.

Any review of files maintained on College equipment, servers and personal computers should only be in accordance with a specific investigation, and where there is reasonable

cause, in the estimation of the College President or the Legal Affairs Office, that evidence will be found, and where the search is limited to locating evidence of misconduct. Prior to the search of files, the computer will be secured and the individual who is the subject of the investigation shall be notified and offered the opportunity to be present during the search.

The College does not monitor or review the content of electronic mail transmissions, files, or other data maintained in its computing resources, except as stated below.

Monitoring may occur in connection with a specific investigation of the violation of law or College policy and when there is reasonable cause, in the estimation of the College President or the Legal Affairs Office, to believe that the user is committing such a violation.

Monitoring can also occur of the applications currently in use, not the content, if technology staff reasonably suspects that College rules are being violated.

Technology staff may also inadvertently compromise privacy during routine network performance monitoring or troubleshooting, or during system maintenance. The number of persons with this level of access will be strictly limited and they have been directed to respect privacy and keep confidential the contents of any message read. However, should this reveal any activity that violates the law or College policy, an investigation will be initiated.

In addition, during the absence of an individual, it may be necessary to access the computer assigned to them in order to conduct the ordinary business of the College. In such instances, the supervisor may request that the Office of Desktop Services provide such access, and a representative of the Legal Affairs Office must be present.

Violations

Users who do not observe these standards are subject to restriction or loss of computing privileges, and could be subject to civil and criminal penalties. Disciplinary sanctions will be subject to the procedures set forth in the respective bargaining agreements.

The College reserves the right to take down or block access to sites within its domain when a claimed copyright infringement has been formally received as per the Digital Millennium Copyright Act of 1998. Upon receipt of a notification claim, the College will notify the site's author and expeditiously remove access to the site containing the material claimed to be in violation. The site will remain off-line until such time that the site author removes the material in question, obtains permission to display the material from the copyright holder or provides proof that the material does not infringe upon the copyright of another. The College reserves the right to terminate the accounts of individuals who are found to be repeat infringers.

Board of Trustees
February 1, 2002