INFORMATION TECHNOLOGY POLICIES and GUIDELINES
For guests

Suffolk County Community College, in its discretion, may permit access to certain computing resources by community residents. These computing resources may include, but are not limited to, host computer systems, Internet access, personal computers and peripherals, software and data files. None of these facilities are provided for sending or receiving private or confidential electronic information. Web site hosting is not available.

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

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.
2.

Privacy Policy

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. As such, it may be subject to subpoena or an application to review records under the Freedom of Information Law, 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.

Monitoring

It is not the College's practice to monitor the content of electronic mail transmissions, files, or other data maintained in its computing resources. Certain limitations to this general philosophy are, however, indicated.

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

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 Legal Affairs Office, to believe that the suspect 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. Should this reveal any activity that violates the law or College policy, an investigation will be initiated. 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.

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 taken in accordance with the procedures set forth in the Student Code of Conduct (or any code adopted applicable to guests), and can include interim sanctions that may involve removal of computer use privileges of those suspected of violating this policy.

Board of Trustees
February 1, 2002