

CAP # 1.2 Network, Internet and Lab Acceptable Use Revision Date: July 2006

Employee: Please read both pages, complete the second page and forward the original to Information Systems, Building A, Suite 122, ATTN: Help Desk.

I. Definition: Purpose of Network

The purpose of the Chipola College (CC) computer network is to support the mission and goals of Chipola College by enhancing both internal and external communication and providing access to a wide range of information sources including the Internet. Use of the CC network and the Internet is a privilege, not a right. To maintain this privilege, users of the network, Internet and labs are responsible for following both the letter and the spirit of this acceptable use policy in order to maintain a usable computing environment for all users.

II. Authorized Users

The CC network is for the exclusive use of full- and part-time faculty, currently enrolled students, and full- and part-time staff of Chipola College. A current, valid student I.D. may be required to gain access to certain facilities. Community members may be given limited access to certain facilities for a fee. Chipola College retirees may be granted access to certain facilities as well.

- Access numbers, I.D.s or accounts on computing systems will be provided to students, faculty, and staff of the college according to the
 procedures outlined below. Access to these systems is granted solely for the pursuit of scholarly activity and/or other activities related directly
 to the mission of the college. Access to these systems is granted subject to adherence to generally accepted ethics. Unapproved or unethical
 use of such access may be grounds for revocation of this access. All requests for access numbers, I.D.s, and accounts will be maintained on
 file.
- 2. Access to computing systems for students will be granted for the duration of an academic term. At the beginning of the succeeding term, all student accounts and associated data and program files associated with these accounts will be purged. Prior to purging any accounts, a complete backup of the affected data and program files will be performed. Dormant accounts will be subject to purge. Periodic monitoring of system and storage use may be performed to identify abnormal use patterns. Exceptions to this policy are handled on a case-by-case basis.
- 3. Access to computing systems for faculty and staff will be granted for the duration of the faculty or staff member's employment and will be removed when employment is terminated. Periodic monitoring of system and storage use may be performed to identify dormant accounts as candidates for removal from the system.
- 4. Authorized personnel within a department may request user I.D.s and sign-ons for student employees. However, the authorized individual will be responsible for verifying that the student employee's access level is no greater than the minimum required to perform the duties of the position.
- 5. All computer accounts will be password protected and holders of these accounts are advised to change passwords when they first receive the account and on a frequent basis thereafter. A password may be reset with appropriate authorization and/or authentication.

III. Definition of Privileges

- Network users have access to those resources and services on the network and through the Internet or other online services that are appropriate and/or are necessary to their job function or course of study.
- 2. At Chipola College, the user is free to pursue knowledge in areas which he or she has special training and preparation and to convey that knowledge to others. Among employees and associates of the college there must be no attempted intimidation by word or deed of those with differing views and methods when they are consistent with professional ethics.
- E-mail communications, documents, or other materials resident on the network are the property of Chipola College and the college retains the right to review these communications or materials. The network administrator may delete any information which violates the college's standards.

IV. Definition of Responsibility

- Network etiquette –All users of the network, Internet or other online services are expected to abide by generally accepted rules of network
 etiquette and the general policies of the College. Use of other organizations' networks or online services through the CC network must comply
 with the rules for that network.
- 2. **Security** All individual computer accounts (sign-ons) are for the use of a single individual, the person for whom the account was approved. Users of the network, Internet or other online services are responsible for protecting the security of the network by keeping passwords confidential, not using another user's account nor loaning accounts, and reporting any security problems to the network administrator.
- 3. Prohibited uses –The college does not condone illegal, abusive, or wasteful use of any public resources, including computers and video, voice, and/or data networks. In that sense, information technologies are no different from any other college resource. Use of the network or the Internet or other online services in violation of local, state or federal law or regulations, or Policy and Procedure is prohibited. Prohibited



use includes, but is not limited to, copyright infringement, fraud, forgery, harassment, slander, or disruption of service. Laws and regulations relevant to prohibited uses include the following:

- Florida computer crimes statute (FS 815)
- statutes prohibiting trafficking in child pornography
- statutes and standards prohibiting sexual harassment in the work place
- laws and rules against use of state resources for private purposes
- acceptable use standards for any network used (e.g. Internet service providers, Freenets, etc.)
- Use of the network or the Internet or other online services for commercial, political or other personal use not related to the support of the mission and goals of Chipola College is prohibited.
- Providing direct hypertext links on a college Web site to potentially offensive materials (e.g. sexually explicit displays, web sites that are overtly racist, etc.), even though the sources themselves are not a part of the college information resources environment, is prohibited
- Use of information technologies to create and/or abet a situation of sexual harassment is prohibited.
- Attempting to circumvent established security procedures or obtain access to privileges to which a user is not entitled is prohibited. d.
- Unauthorized access, alteration or destruction of another user's data or programs is prohibited.
- Installing or downloading software to the local hard drive of a workstation without authorization is prohibited.
- Any unauthorized, deliberate action which intentionally damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.
- Viewing sexually explicit material is prohibited.

V. Disclaimers

Chipola College does NOT warrant that the functions of this system will meet any specific requirements users may have nor that it will be error free or uninterrupted. Nor shall it be liable for any indirect, incidental or consequential damages (including lost data, information or profits) sustained or incurred in connection with the use, operation or inability to use the system.

Internet and other online access is provided by the Chipola College network. However, the college has no control over the content of the Internet or other online services, some of which may be deemed controversial or offensive by the individual user. Chipola College specifically disclaims any warranty as to the information's accuracy, authoritativeness, timeliness, usefulness or fitness for a particular purpose. Chipola College shall have no liability for any direct, indirect or consequential damages related to the use of the information contained on the Internet or other online services. If such an event should occur, this organization will fully comply with the authorities to provide any information necessary for the litigation process.

VI. Penalties for Violation of Policy

Failure to abide by the Network, Internet and Lab Use Acceptable Use Policy, can result in immediate loss of network privileges, including deletion of user accounts and/or other disciplinary or legal action.

I understand and will abide by the above terms and conditions for use of these facilities and services. If the propriety of any situation is unclear, I

will ask for clarification from the network administrator father than making any assumpt	IOLIS.
Last Name (UPPERCASE) First Name (UPPERCASE)	Department Contact Name: Phone Number:
Social Security # XXX - XX -	
Signature	Date
Please mark the appropriate employing agency, classification, department:	
Student	OTHER Community User
As: Administration Faculty Career Service OPS	Adjunct (For adjunct faculty, the gray section below should be completed by your supervisor.)
Dept: Bldg/Room #:	Office Phone:
DEPARTMENT SUPERVISOR USE	
INFORMATION PERTAINING TO ADJUNCT INSTRUCTORS: Adjunct instructors are part-time, temporary employees, non-Career Service. At this form's submission to Information Systems. An adjunct's network account	

must authorize an adjunct's network account to be extended to the next term. An e-mail account for an adjunct will be created when the department supervisor requests it.

CREATE E-MAIL ACCOUNT FOR ADJUNCT:	YES	NO		
DEPARTMENT SUPERVISOR'S SIGNATURE:				