North Florida Community College

North Florida Community College Computer and E-mail Usage

Acceptable Use Policy

Introduction

As part of its educational mission, North Florida Community College acquires, develops, and maintains computers, computer systems and network. These computing resources are intended for college-related purposes, including direct and indirect support of the college's instruction, research and service missions; college administrative functions; student and campus life activities; and the free exchange of ideas within the college community and among the college community and the wider local, national and world communities.

This policy applies to all users of college computing resources, whether affiliated with the college or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may govern specific computers, computer systems or networks provided or operated by specific units of the college.

Rights and Responsibilities

The rights of academic freedom and freedom of expression apply to the use of college computing resources. So too, however, do the responsibilities and limitations associated with those rights. The college supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of college computer resources, like the use of other college-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

General Rules

Users of college computing resources must comply with federal and state laws, college rules and policies, and the terms of applicable contracts including software licenses while using college computing resources. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Florida Computer Crimes Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which

prohibit “hacking”, “cracking” and similar activities; the college’s Student Code of Conduct; the college’s Sexual Harassment Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or network may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using college computing resources. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate network administrator and/or Dean, Director or Department Chair.

Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of college computing resources, the college may require users of those resources to limit or refrain from specific uses if, in the opinion of the system administrator, such as interferes with the efficient operations of the system.

Users may not state or imply that they speak on behalf of the college or use college trademarks and logos without authorization to do so. Authorization to use college trademarks and logos on college computing resources may be granted only by the Office of College Advancement. The use of appropriate disclaimer is encouraged.

Users must not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of NFCC computers, networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.

Enforcement

Users who violate this policy may be denied access to college computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violation of applicable law to appropriate law enforcement agencies.

Security and Privacy

The college employs various measures to protect the security of its computing resources and its users’ accounts. Users should be aware, however, that the college cannot guarantee security

and confidentiality. Users should therefor engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them according to college policy.

Users should be aware that their uses of college computing resources are not completely private. While the college does not routinely monitor individual usage of its computing resources, the normal operations and maintenance of the college's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The college may also specifically monitor the activity and accounts of individual users of college computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to Usenet or a Web page:
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability.
- There is reasonable cause to believe that the user has violated or is violating this policy;
- An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Networking Services in consultation with the Dean of Administrative Services. The college, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate college personnel or law enforcement agencies and may use those results in appropriate college disciplinary proceedings. Communications made by means of college computing resources are also generally subject to the Florida Public Records Law to the same extent as they would be if made on paper.

Visitors to NFCC Web sites who are not currently NFCC students, faculty or staff should refer to the college's Internet Privacy Policy for privacy information.

Installation of Software

Users are not authorized to install any software on the college's computers. Installation of software must be done by the Office of Computer Services staff. Usage of "instant messaging", "chat rooms", or other messaging services may interfere, or impair the normal operation of other installed software. Use of messaging programs is prohibited. Downloading and installation of "Shareware" or "Freeware" is prohibited. If the software, add-on, or downloaded program is not licensed and installed by the college, it is unauthorized.

Email

For purposes of this document, email includes point-to-point messages, postings to newsgroups and list servers and any electronic messaging involving computers and computer networks, Organizational e-mail accounts, including those used by student organizations, are held to the same standards as those for individual use by members of the North Florida Community College community. While email may not be used to solicit others for commercial ventures, personal gain, religious or political causes, or other non-business matters, occasional use of emails for public service and the common good is acceptable. Email messages that contain material considered offensive to others are unacceptable. E-mail is also generally subject to the Florida Public Records Law to the same extent as it would be on paper.

Examples of Inappropriate Uses of E-mail

While not an exhaustive list, the following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at North Florida Community College. In general, e-mail shall not be used for the initiation or retransmission of:

Chain mail that misuses or disrupts resources (i.e. e-mail sent repeatedly from user to user, with requests to send to others);

Harassing or hate-mail – any threatening or abusive e-mail sent to individuals or organizations which violate college rules and regulations or the Student Code of Conduct;

- Virus hoaxes;
- Spamming or e-mail bombing attacks – intentional e-mail transmissions that disrupt normal e-mail service;
- Junk mail – unsolicited e-mail that is not related to college business and is sent without a reasonable expectation that the recipient would welcome receiving it: and
- False identification – any actions that defraud another or misrepresent or fail to accurately identify the sender.

Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of college computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other college responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of College equipment.

Web Pages

Official college pages (including colleges, departments, bureaus, centers, institutes, etc.)

represent the college and are intended for the official business functions of the college. Each official home page must use an address that ends in "nfcc.edu" and be registered and published by the college's Web administrator who will then include it as a link from the NFCC web site home listing. Rules, standards and request for publishing pages are available by contacting the Web Master.

Learning Management System

Desire2Learn (D2L) is the supported learning management system for online courses and is available for faculty use in supplementing traditional courses. All NFCC students are provided an email account through D2L, and this is the official email address used by faculty and staff for communication with students. For questions or assistance with D2L, contact the D2L Helpdesk.

Commercial Pages

Using NFCC Web pages for personal gain is forbidden. Any private commercial use of NFCC Web pages must be pre-approved pursuant to existing college policies and procedures regarding outside employment activities. The college may require pages involving commercial use to reside on a specific domain such as nfcc.edu. All NFCC units that accept payment electronically via the Internet are required to process all sales transactions through the Office of Finance and Administration. For advertising, Web page authors should clear any ads with the Office of College Advancement prior to publishing.

External Links

NFCC accepts no responsibility for the content of pages or graphics that are linked from NFCC pages. However, Web page authors should consider that such links, even when clearly labeled, can be misinterpreted as being associated with the College. Links to pages where you have a personal monetary interest are likely to violate policies regarding advertising and commercial use and should be avoided.

Excessive or Disruptive Use

Excessive or disruptive use of college resources in the viewing or publishing of Web pages is not permitted. Units owning or administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive.

Retention Periods

Retention periods must be followed for all official college Web pages as required by the Florida

Public Records Law. Official college Web pages are treated like e-mail and subject to the same guidelines set forth in the NFCC public records policy.

Network Infrastructure/Routing

Users must not attempt to implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to NFCC IT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the Network Services.

Wireless

For the purposes of this document, we refer only to wireless transmission using radio frequency (RF). Wireless is shared media and easily intercepted by a third party. Wireless users are encouraged to use some type of encryption. NFCC provides access to the internet from NFCC wireless connections, but it doesn't provide encryption. For security purposes, wireless users are not allowed to authenticate and connect to the NFCC network.

Improperly configured wireless access points (WAPs) might cause denial of service to legitimate wireless users. WAPs can also be used to subvert security. Wireless access points must be authorized by authorized by Network Services.

General Information

Computers, computer files, the e-mail system, and software furnished to employees, students, and patrons are the property of North Florida Community College and intended for business use only. Users should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer and e-mail usage may be monitored.

North Florida Community College strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, North Florida Community College prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale.

For example, the display or transmission of sexually explicit images and messages is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

E-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters.

North Florida Community College purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, North Florida Community College does not have the right to reproduce such software for use on more than one computer.

Users may only use software on local area networks or on multiple machines according to the software license agreement. North Florida Community College prohibits the illegal duplication of software and its related documentation.

As a safeguard users should store all documents, spreadsheets, and other data in their home folder on the "H" drive. This drive is backed up daily and provides safety and security beyond the capabilities of the local "C" drive.

Users should notify their immediate supervisor, and Computer Services or any member of management upon learning of violations of this policy. Users who violate this policy will be subject to disciplinary action, up to and including termination of employment.

Internet Usage

Internet access to global electronic information resources on the World Wide Web is provided by North Florida Community College to assist employees and students in obtaining work-related data and provide access for educational research. The following guidelines have been established to help ensure responsible and productive Internet usage. While Internet usage is intended for official activities, incidental and occasional brief personal use is permitted within reasonable limits.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of North Florida Community College and as such is subject to disclosure to law enforcement officials and/or third parties. Consequently, employees, students, and patrons should always ensure that information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment services, and technology provided to access the Internet remain at all times the property of North Florida Community College. As such, North Florida Community College reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could offend someone on the basis of race,

age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if a user did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet. Users are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

Abuse of the Internet access provided by North Florida Community College in violation of law or North Florida Community College policies will result in disciplinary action, up to and including termination of employment. Users may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

*Sending or posting discriminatory, harassing, or threatening messages or images
*Using the organization's time and resources for personal gain
*Stealing, using, or disclosing someone else's code or password without authorization
*Copying, pirating, or downloading software and electronic files without permission
*Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
*Violating copyright law
*Failing to observe licensing agreements
*Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions.
*Sending or posting messages or material that could damage the organization's image or reputation
*Participating in the viewing or exchange of pornography or obscene materials
*Sending or posting messages that defame or slander other individuals
*Attempting to break into the computer system of another organization or person
*Refusing to cooperate with a security investigation
*Sending or posting chain letters, solicitations, or advertisements not related to business purposes or educational activities
*Using the Internet for political causes or activities, religious activities, or any sort of gambling
*Jeopardizing the security of the organization's electronic communications systems
*Sending or posting messages that disparage another organization's products or services
*Passing off personal views as representing those of the organization
*Engaging in any other illegal activities