

BOBCAT COMPUTING

Policy

The overarching policy governing computing and networking at Jones is the Policy on Acceptable Use of Electronic Resources. The policy is reprinted in its entirety below. Faculty, staff, and students are urged to review and understand the contents of this policy. Violations of the policy may result in sanctions up to and including termination or expulsion.

Policy on Acceptable Use of Electronic Resources

Summary

This policy defines the boundaries of "acceptable use" of College electronic resources, including computers, software, networks, electronic mail services and electronic information sources. This policy contains specific rules that can be modified as the electronic information environment evolves.

This policy is based on the principle that the electronic information environment is provided to support College business and its mission of education and service while other uses are considered secondary. Some uses of the electronic information systems are forbidden such as:

- uses that threaten the integrity of the system;
- uses that threaten the function of non-College equipment that can be accessed through the system;
- uses that threaten the privacy of others;
- uses that threaten the actual or perceived safety of others;
- uses that are otherwise illegal.

By using College electronic information systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable College policies, as well as State and Federal laws and regulations. Use of facilities may be subject to monitoring for appropriate purposes.

This policy defines penalties for infractions, up to and including loss of system access, employment termination or expulsion. In addition some activities may lead to risk of legal liability, both civil and criminal.

Users of electronic information systems are urged in their own interest to review and understand the contents of this policy.

Purposes

Jones County Junior College makes computing resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, software, electronic information and data) available to faculty, students, staff, affiliates, registered guests, and the general public to support the educational, research and service missions of the College.

Priorities for the use of computing resources will be established and enforced. The priorities for use of College-wide computing resources are:

- 1) Uses that directly support the educational and service missions of the College.
- 2) Other uses that indirectly benefit the education and service missions of the College, as well as and including reasonable and limited personal communications.

Implied Consent

Each person with access to the College's computing resources is responsible for his or her appropriate use. By their use each person agrees to comply with all applicable College and departmental policies and regulations, and with applicable State and Federal laws and regulations, as well as with the acceptable use policies of affiliated networks and systems.

Academic Freedom and Responsibility: The rights of freedom of thought, inquiry and expression, as defined in the College's Policy and Procedure Manual (Section 401.5), are paramount values of the College community. The College's commitment to the principles of open expression extends to and includes the electronic information environment, and interference in the exercise of those rights is a violation of this policy and of the policies in the Jones Policy and Procedure Manual.

General Standards for the Acceptable Use of Computer Resources: Failure to uphold the following General Standards for the Acceptable Use of Computer Resources constitutes a violation of this policy and may be subject to disciplinary action.

The General Standards for the Acceptable Use of Computer Resources require:

- Responsible behavior with respect to the electronic information environment at all times;
- Behavior consistent with the mission of the College and with authorized activities of the College or members of the College community;

- Compliance with all applicable laws, regulations, and College policies;
- Respect for the principles of academic freedom and responsibility;
- Truthfulness and honesty in personal and computer identification;
- Respect for the rights and property of others, including intellectual property rights;
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and
- Respect for the value and intended use of human and electronic resources.

Enforcement and Penalties for Violation: Any person who violates any provision of this policy, of the Specific Rules interpreting this policy, of other relevant College policies, or of applicable State or Federal laws or regulations may face sanctions up to and including termination or expulsion. Depending on the nature and severity of the offense, violations can be subject to disciplinary action through the Vice President of Student Affairs or disciplinary procedures applicable to faculty and staff.

It may at times be necessary for authorized systems administrators to suspend someone's access to College computing resources immediately for violations of this policy, pending interim resolution of the situation. In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.

System owners, administrators or managers may be required to investigate violations of this policy and to ensure compliance.

Amendment

Formal amendment of the General Standards of Acceptable Use of Computing Resources or other aspects of this policy may be promulgated by the Network Services Manager & Computer Services Director following consultation with the Technology Resource Management Steering Committee. If and when changes are made appropriate effort such as posting changes on the College's web page and placing a notice in the school newspaper will be made to notify the College community.

Interpreting This Policy

As technology evolves, questions will arise about how to interpret the general standards expressed in this policy. The Network Services Manager & Computer Services Director shall, after consultation with the Technology Resource Management Committee publish specific rules interpreting this policy.

Specific Rules Interpreting the Policy on Acceptable Use of Electronic Resources

The following specific rules apply to all uses of College computing resources. These rules are not an exhaustive list of proscribed behaviors, but are intended to implement and illustrate the General Standards for the Acceptable Use of Computer Resources, other relevant College policies, and applicable laws and regulations. Departments and system administrators may promulgate additional specific rules for the acceptable use of individual computer systems or networks.

Content of Communications

- c Except as provided by applicable State, or Federal laws, regulations or other College policies, the content of electronic communications is not by itself a basis for disciplinary action.
- c Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law), are prohibited.
- c The use of College computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable College policies) are prohibited.

Identification of Users

Anonymous and pseudonymous communications are not permitted except when expressly approved by the operating guidelines or stated purposes of the electronic services to, from, or through which the communications are sent. However, when investigating alleged violations, the Technology Resource Management Committee may direct the Network Services Manager & Computer Services Director, or an authorized system administrator, to attempt to identify the originator of anonymous/pseudonymous messages, and may refer such matters to appropriate disciplinary bodies to prevent further distribution of messages from the same source.

The following activities and behaviors are prohibited:

- c Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication;

- c Acquiring or attempting to acquire passwords of others;
- c Using or attempting to use the computer accounts of others;
- c Alteration of the content of a message originating from another person or computer with intent to deceive; and
- c The unauthorized deletion of another person's news group postings.

Access to Computer Resources

The following activities and behaviors are prohibited:

- c The use of restricted-access College computer resources or electronic information without or beyond one's level of authorization;
- c The interception or attempted interception of communications by parties not explicitly intended to receive them;
- c Making College computing resources available to individuals not affiliated with Jones County Junior College without approval of an authorized College official;
- c Making available any materials the possession or distribution of which is illegal;
- c The unauthorized copying or use of licensed computer software;
- c Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the College's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records, or as defined by the cognizant Security Officer;
- c Intentionally compromising the privacy or security of electronic information; and
- c Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).

Operational Integrity

The following activities and behaviors are prohibited:

- c Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts;
- c Failure to comply with requests from appropriate College officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
- c Revealing passwords or otherwise permitting the use by others (by

intent or negligence) of personal accounts for computer and network access;

- c Altering or attempting to alter files or systems without authorization;
- c Unauthorized scanning of networks for security vulnerabilities;
- c Attempting to alter any College computing or networking components (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one's level of authorization;
- c Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;
- c Intentionally disrupting the use of electronic networks or information systems;
- c Intentionally wasting human or electronic resources; and
- c Negligence leading to the damage of College electronic information, computing/networking equipment and resources.

Appendices

Relevant College Policies

The use of computing resources is also required to conform to the following College policy:

Code of Student Conduct

In addition, specific policies of the College's Schools, departments, computer systems and networks, and other general College policies and regulations are also applicable to the use of computer resources. These policies include, but are not limited to, the following:

- c Patent Policy
- c Copyright Policy
- c Computer Software Policy
- c FERPA

Applicable Laws

Computer and network use is also subject to Mississippi and Federal laws and regulations. Suspected violations of applicable law are subject to investigation by College and law enforcement officials. Among the applicable laws are:

Federal Copyright Law: U.S. copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display,

attribution and integrity to their creations, including works of literature, photographs, music, software, film and video.

Violations of copyright laws include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recordings) and distributing copyrighted materials over computer networks or through other means.

Federal Wire Fraud Law: Federal law prohibits the use of interstate communications systems (phone, wire, radio, or television transmissions) to further an illegal scheme or to defraud.

Federal Computer Fraud and Abuse Law: Federal law prohibits unauthorized access to, or modification of information in computers containing national defense, banking, or financial information.

Federal Child Pornography Laws: Federal laws prohibit the creation, possession, or distribution of graphic depictions of minors engaged in sexual activity, including computer graphics. Computers storing such information can be seized as evidence. Child pornography is absolutely against the law. It is a violation of Federal free/statutes to transmit this material across state lines, even electronically, and certain obscene materials are in violation of the Mississippi Code. (References: <http://www.mscode.com/free/statutes/97/005/0029.htm> and <http://www.mscode.com/free/statutes/97/029/0101.htm>)

Pyramid schemes/Chain Letters: It is a violation of the Federal Postal Lottery Statute to send chain letters that request sending money or something of value through the U.S. mail. Solicitations through electronic messaging are also illegal, if they require use of U.S. Mail for sending money/something of value.

Defamation: Someone may seek civil remedies if they can show that they were clearly identified as the subject of defamatory messages and suffered damages as a consequence. Truth is a defense against charges of defamation.

Common law actions for invasion of privacy: Someone may seek civil remedies for invasion of privacy on several grounds.

Public disclosure of private facts: the widespread disclosure of facts about a person, even when true, may be deemed harmful enough to justify a law suit.

False light: a person wrongfully attributes views or characteristics to another person in ways that damage that person's reputation.

Wrongful intrusion: the law often protects those areas of a person's life in which they can reasonably expect they will not be intruded upon.

MISSISSIPPI LAWS THAT APPLY TO THE USE OF COMPUTING AND NETWORKING SYSTEMS AND TO PUBLICLY ACCESSIBLE WEB PAGES

The following are examples of violations of the laws of the State of Mississippi (Mississippi Code of 1972 -

<http://www.mscode.com/free/statutes/97/045/0011.htm>):

Public display of sexually oriented materials in a venue likely to be visited by minors in the normal course of business. (Reference:

<http://www.mscode.com/free/statutes/97/005/0029.htm>)

Intentional deceit of anyone as to your true identity for the purpose of obtaining anything of value. You should not use someone else's e-mail account at all, but to do so for personal gain is illegal. (Reference:

<http://www.mscode.com/free/statutes/97/019/0085.htm>)

Profane or indecent language in a public place. A web page that resides on a College server is a public place. (Reference:

<http://www.mscode.com/free/statutes/97/029/0047.htm>)

Publishing or exhibiting obscene materials. (Reference:

<http://www.mscode.com/free/statutes/97/029/0101.htm>)

Hacking or passing along hacker information concerning a computer, computer system, or network to another person. Obtaining services to which you are not entitled and either inserting or changing system files are all illegal. (Reference:

<http://www.mscode.com/free/statutes/97/045/0003.htm>)

Blocking another user from using a system he/she is entitled to use.

(Reference: <http://www.mscode.com/free/statutes/97/045/0005.htm>)

Using or sharing the results of cracking a password file. This may result in up to five years in jail and a fine of up to \$10,000. (Reference:

<http://www.mscode.com/free/statutes/97/045/0005.htm>)

Intentional modification or destruction of computer equipment or supplies. (Reference: <http://www.mscode.com/free/statutes/97/045/0007.htm>)

Erasing, modifying, sharing, or using the information in the files of another user. (Reference: <http://www.mscode.com/free/statutes/97/045/0009.htm>)

All of the activities outlined in the Mississippi Code are unlawful if the user was physically in Mississippi when the act was committed, was committing the act against a computer or system in Mississippi, or used a computer or network in Mississippi as a relay point. (Reference:

<http://www.mscode.com/free/statutes/97/045/0011.htm>)

Jones Junior College

ELECTRONIC USE POLICY

2010-11