



ADMINISTRATIVE POLICY	
Policy Type:	Responsible Use
Date Adopted:	December 18, 2003
Date Last Reviewed:	December 18, 2003
Responsible Office:	Information Technology

Summary: This policy is designed to indicate what is considered responsible use of information technology resources. It includes eight key sections that protect the college, inform users, and maintain system integrity/performance for all users. Use of any institutional information technology resource acknowledges acceptance of the Responsible Use Policy.

Table of Contents:

Topic	Page
1. DEFINITIONS:	1
2. POLICY:	1
3. EXPECTATIONS OF PRIVACY:	2
4. RESPONSIBILITIES:	2
5. PROHIBITED CONDUCT:	3
6. REPORTING INCIDENTS:	4
7. SANCTIONS:	4
8. EXTERNAL NETWORKS:	4

1. Definitions:

- 1.1. The term “College” means Jackson Community College including all its extension centers and all other Jackson Community College supported operations and events.
- 1.2. The term “user” means any employee, student, guest, or agent who accesses Jackson Community College resources on or off campus.
- 1.3. The phrase “information technology resources” means data in any medium such as digital, video, audio, or paper; any hardware and software applications that access information; any network systems that transport information that are owned by the College or are in the College’s possession, custody, or control.

2. Policy:

- 2.1. Jackson Community College provides information technology resources for the use of students, staff, faculty, and authorized guests in performing educational, scholarly, cultural, or other tasks that further the college mission.
- 2.2. Users of information technology resources must comply with all federal, state, and other applicable laws. Examples of federal, state, and local law include, but are not limited to: libel, privacy, copyright and fair use, trademark, obscenity, the Electronics Communications Privacy Act, the Computer Abuse and Fraud Act, the Freedom of Information Act. Additional examples include requirements for the provision of employment and educational environments free from race-based or gender-based hostility; laws prohibiting harassment; laws prohibiting the exhibition of obscene materials to minors.

- 2.3. Users of information technology resources must comply with College regulation and policy; all applicable contracts and licenses; and maintain the highest standards of ethics and professional conduct. Examples of such rules, policies, and licenses include, but are not limited to the College student code of conduct; College sexual harassment policy; all applicable software licenses and any rule/policy/law not expressly referenced in this policy.
- 2.4. Users are responsible for understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their uses. In cases of doubt the burden of responsibility is on the user to inquire about the permissibility of an action or use prior to execution.
- 2.5. Nothing in this policy prohibits the use of appropriate material for educational purposes in an educational program in which a minor is participating. Nothing in this policy prohibits the presence of minors at an exhibition or display or the use of any material in any public library.
- 2.6. Jackson Community College extends the privilege of membership in the electronic community to students, employees, and community partners with the stipulation that they be responsible citizens. The College computing community is based on a spirit of mutual respect to create a community of responsible users.

3. Expectations of Privacy:

- 3.1. Users are advised that the College is entitled to access and to monitor its information technology resources without prior notice, knowledge or permission for any purpose permitted by law including, but not limited to, complying with a court order, warrant, subpoena, or other legal discovery request for information; assessing compliance with College policies or any applicable law; preserving property or information; maintenance, security or safety concerns; resolving urgent incidents; obtaining valuable College information. The College advises users that access and monitoring is a reasonable means of protecting and advancing College resources and users should have no expectation of privacy in information stored on or transmitted over the College's information technology resources.
- 3.2. Users are advised of computer monitoring via login notification coordinated by the Director of Information Technology. Data will not be used for evaluation or punitive purposes without the knowledge of the user; evaluation/punitive proceedings will follow employment contracts or stated student rights and responsibilities.
- 3.3. The College can disclose information or communication to law enforcement or investigative authorities or to comply with Freedom of Information Act requests, without the authorization of the user and without authorization by the sender or any other party to the information or communication.
- 3.4. The College advises users that Internet sites they visit and information/graphics they download are able to be documented by the College's network management. Users are also advised that deleting an electronic communication item is not effective as numerous copies are stored in a system.

4. Responsibilities:

- 4.1. User Responsibilities
 - 4.1.1. Use resources only for authorized purposes as defined in Section 1.
 - 4.1.2. Access only files and data that are your own, that are publicly available, or to which you have been given authorized access.
 - 4.1.3. Protect your user id and password from unauthorized use. You are responsible for all activities on your user id.
 - 4.1.4. Use only legal versions of copyrighted software in compliance with vendor license requirements.

- 4.1.5. Use scanners, photocopiers, or other recording devices and media in a manner consistent with copyright law, including Fair Use.
- 4.1.6. Refrain from monopolizing systems; overloading networks with excessive data; use of excessive disk space, printer or copier paper.
- 4.1.7. Report alleged violations of the Responsible Use Policy as specified in Section 6.
- 4.1.8. Comply with all rules and laws as specified in Section 1.
- 4.1.9. Inform non-College e-mail correspondents that e-mail received by the College information technology systems becomes property of the College.

4.2. Service Provider (Information Technology) Responsibilities

- 4.2.1. Offer timely and efficient service while considering the needs of the total user community.
- 4.2.2. Report all incidents as specified in Section 6.
- 4.2.3. Monitor network activity, suspend access, and/or preserve files when requested or in order to forestall an immediate threat to the system or its users.
- 4.2.4. Follow the same policies and conditions of use that other users must follow.

4.3. College Responsibilities

- 4.3.1. Protect against damage to College information technology resources.
- 4.3.2. Safeguard the integrity of computers, networks, software, and data.
- 4.3.3. Preserve information and data.
- 4.3.4. Maintain or upgrade information technology resources.
- 4.3.5. Investigate the posting of proprietary software or electronic copies of texts, data, media, or images in disregard of copyright, license, or other contractual obligation or in violation of law.
- 4.3.6. Comply with court orders, subpoenas or other legally enforceable discovery requests.
- 4.3.7. Protect the College or its employees or representatives against liability and other potentially adverse consequences.

5. **Prohibited Conduct:**

5.1. Jackson Community College designates the following activities as unethical, unacceptable, and cause for disciplinary or legal action:

- 5.1.1. Using another person's/institution's user id or password unless authorized by administration.
- 5.1.2. Using computer applications or any device to decode passwords or access control information.
- 5.1.3. Attempting to circumvent or subvert system security measures.
- 5.1.4. Engaging in any activity that might be harmful to information technology resources including, but not limited to, chain mail, propagating viruses, setting up servers to download and/or share files, using excess bandwidth, damaging files.
- 5.1.5. Using information technology resources to encourage circumvention of Responsible Use.
- 5.1.6. Using information technology resources for personal profit or promoting or advertising business.
- 5.1.7. Using information technology resources for political or religious purposes without authorization from the College president or his/her designee.
- 5.1.8. Using, making, storing, or transmitting copies of data, audio, or media files or applications that violate copyright law.
- 5.1.9. Using information technology resources to harass or intimidate another person.
- 5.1.10. Monopolizing information technology resources.
- 5.1.11. Violating any local, state, or federal law (e.g. viewing child pornography, hacking systems internal or external to the college, conducting illegal transactions of stolen or illicit goods, etc.).

5.2. Employees are prohibited from accessing, storing, or transmitting obscene material (as defined by applicable law and/or community standards) while on College premises or utilizing College

information technology resources (e.g. MichNet/Merit accounts) except in cases where the material is being used in a College educational program. See Section 1: 1.2 and 1.5.

- 5.3. In order to ensure College operations, the College administration may access employee files and data with authorization from the College president or his/her designee.

6. Reporting Incidents:

- 6.1. Alleged incidents involving students should be reported to the Dean of Student Services.
- 6.2. Alleged incidents involving employees or community partners should be reported to the Executive Director of Human Resources.
- 6.3. Violations of this policy are prohibited and may also be violations of other College policy and in some cases may constitute criminal offenses. You are asked to report information you may have concerning instances in which this policy has been or is being violated.

7. Sanctions:

- 7.1. Students who engage in any activity that violates the Responsible Use Policy are subject to disciplinary action pursuant to the process outlined in the Student Rights and Responsibilities Handbook, which provides for a range of sanctions including expulsion.
- 7.2. Represented employees who engage in any activity that violates the Responsible Use Policy are subject to disciplinary action pursuant to the applicable collective bargaining agreements. Violation of the Responsible Use Policy is a violation of College policy.
- 7.3. Non-represented employees who engage in any activity that violates the Responsible Use Policy are subject to disciplinary action pursuant to College policy.
- 7.4. In accordance with established College policies and practices, confirmation of inappropriate use of information technology resources may result in termination of access, disciplinary review, expulsion, termination of employment, legal action, or other disciplinary action. Information Technology staff will work with other College offices or appropriate external agencies in the resolution of problems.

8. External Networks:

- 8.1. External networks to which the College maintains connections (e.g., MichNet/Merit) have established acceptable use standards. It is the responsibility of the user to adhere to the standards of such networks. In cases of doubt, the burden of responsibility is on the user to inquire about external network uses. The College cannot and will not extend any protection to any user who violates the policies of an external network. Michnet/Merit use standards are currently available at <http://www.merit.edu/>

Jackson Community College reserves the right to modify or amend this policy at any time with or without prior notice.