Administrative Policy

Policy Title:	Responsible Use Policy
Policy Number:	LC-1601
Date Adopted:	12/18/2003
Version:	3.0
Review Cycle:	Biennially
Date Last Reviewed:	7/13/2016
Office Responsible:	Information Technology
Reviewing Committee:	NA
Related Policies:	Mass E-mail Policy, Accounts Policy, Student Records, Employee Records, Social Security Number Protection.
Related Laws:	Notification of Rights Under FERPA, Social Security Privacy Act, FOIA

Policy Summary:

The purpose of this policy is to outline the ethical and acceptable use of information technology (IT) resources at Jackson College (JC). These rules are in place to protect users and to ensure that everyone has access to reliable services that are safe from unauthorized or malicious use. Insecure practices and malicious acts expose JC and users to risks including virus attacks, identity theft, compromised network systems, and loss of data.

Scope:

The Responsible Use Policy (RUP) applies to employees, students, and partners as well as any other individuals or entities that use IT resources (hereby referenced as users). This policy applies to all equipment owned or leased by JC. This policy also applies to any privately owned equipment connected to or through IT systems which include, but is not limited to, computer equipment, peripherals, software, operating systems, servers, storage media, networks, and the Internet.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the college community who accesses and uses information technology.

Therefore, every user of college resources is required to know the policies and to conduct their activities within the scope of the RUP. Failure to comply with this policy may result in loss of computing privileges and/or disciplinary action.

Policy Statement:

1. Privacy and Confidentiality

JC desires to provide the highest level of privacy possible for users of its IT systems and to assure their rights of free speech and intellectual freedom are protected and uninhibited. At the same time JC is required by federal and state laws to keep certain information confidential. To the extent permitted by law and college policy, JC maintains and protects both the privacy of individuals and the confidentiality of official information stored on or passing through its IT systems. Privacy and confidentiality must be balanced with the need for the college to manage and maintain networks and systems against improper use and misconduct. All users must understand that data traversing or stored in JC systems are subject to disclosure requests under public records law, under subpoena, and in the e-discovery process in litigation. In order

to comply with the law, college officials may have direct access to stored and or/transient information as provided below.

2. Exceptions to Privacy of Information

As part of their assigned responsibilities, JC employees may have access to confidential information and are restricted to using it only for purposes associated with the requirements of their position. JC may preserve, access, monitor, or disclose confidential or personal information residing on its information networks and systems in the following situations:

2.1 State and Federal Law

All information including the personal, academic, or research data and files residing on college systems is subject to state and federal laws and regulations requiring its disclosure.

2.2 Access to User Accounts to Conduct Business

When the individual is not available but access is needed to their account to conduct college business. Approval to access the account should be given by written recommendation and justification by the individual's supervisor then Human Resources.

2.3 Investigations

During the course of an investigation of misconduct, violations of law, or violations of college policy.

2.4 Maintenance of Jackson College Networks and Systems

To maintain its IT systems to; audit networks and systems on a periodic basis to ensure compliance with security policies; locate and resolve security breaches or other situations that potentially impact the reliability, robustness, or security of the IT infrastructure. Individuals performing these functions or others may have access to personal and confidential information and are restricted to using it only for purposes associated with their position.

2.5 Legal Disclosure Requests

In response to a lawfully issued records request, subpoena, court order or other compulsory legal process ("disclosure request"). To the extent possible and practical, the account holders for e-mail and electronic files will be notified in advance of access or disclosure.

2.6 Health and Safety Emergency

Information necessary and relevant to addressing an emergency situation in order to protect, secure, or triage users.

3. Protection of Information and Security Practices

The development of policy and practices to protect information and to increase security of IT resources is an ongoing process. This document is used to identify key security issues for which users responsible.

3.1. Protection of Information

In a college environment users create, store and have access to many sources of information. The level of security practices required for various information types depends on who has created the information, who is maintaining the information, the nature of the information itself, and whether there are specific federal and/or state laws or college requirements or guidelines associated with the use and distribution of the information. Information can be defined very

generally in many ways such as public, private, confidential, personal, academic, etc. For the purposes of this policy, information is categorized as either college information or individual information. Within college information, there are also very specific definitions for certain types of information.

3.1.1. College Information

As an institution, the college has many types of official information including student records, financial records, health and insurance records, personnel records, and other business records. Departments and other areas may have other types of internal business information specific to their needs.

- Confidential information is defined by federal and/or state law and college policy and includes information such as student educational records, personnel information; financial information, and health and insurance records. All users are responsible for knowing and complying with college policies that apply to confidential information. See Notification of Rights Under FERPA and policies on Student Records, Employee Records, and Social Security Number Protection.
- Business information includes all other information created and maintained for the purpose of operating the college. All employees are responsible for knowing and complying with college policies that apply to business information.
- The college is responsible for securing confidential and business information maintained on the systems under their authority as required by federal and/or state law and college security policy. In addition, they are responsible for developing appropriate security practices for their internal business information.
- Users are responsible for accessing only that confidential or business information for which they are authorized and using that information only for the purposes for which it is intended.
- Users are required to comply with security practices established at the college and departmental level to protect confidential or business information.

3.1.2. Individual Information

Individual information includes academic, research, personal and business correspondence, and other records created and managed by individual users. As creators and managers of this information, individuals are responsible for securing and protecting their information.

Individual information should be protected based on the level of risk associated with its loss or misuse. Users are ultimately responsible for securing their own information and should take action to assure their individual data is protected to the level they or the college deems adequate.

3.2. Password Security

Users are responsible for the security of their JC usernames and passwords and student/employee identification number and will be held accountable for any activities linked to their accounts. Users must follow established college standards for maintaining and managing passwords. Usernames and passwords are never to be shared. Users that suspect their account may have been breached must notify the JC Solution Center immediately.

3.3. User Security Practices

Users are required to be aware of and employ security practices established by the college or department to prevent unauthorized access to their computers. Security breaches can often be

linked to the actions individuals take or fail to take when using IT resources (e.g., leaving their computers logged into applications while away from their desks, storing written copies of passwords in obvious places, using insecure methods for transferring information).

3.4. Security for IT Systems

Computer systems can become transmitters of viruses, denial of service attacks, spam relays, and other malicious electronic activities. E-mail messages, websites, instant messaging, and other applications utilized by users are often the sources of these problems. To prevent these malicious activities, individuals are required to be aware of and comply with college policies relating to the use of these applications. Among specific requirements are the timely acceptance and application of security patches and upgrades to operating systems and other software, reporting possible malware or viruses and prompt implementation of security measures directed by the college or department to specific security threats. Do not download a software program, open an e-mail, or click on a web link if you are uncertain of its authenticity.

3.5. Reporting Security Breaches

Effective security practice includes the prompt and appropriate response to breaches in security. It is, therefore, incumbent upon all individuals to report incidents in which they believe computer or network security has been jeopardized. In some cases local action is sufficient; in others, where the risk to confidential information or college-wide security is high, a college-level response will be implemented.

4. Unacceptable Use

Users are prohibited from engaging in any activity illegal under local, state, federal, or international law or in violation of college policy. The categories and lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.1. Excessive Non-Priority Use of Computing Resources

Priority for the use of information technology resources is given to activities related to the college's missions of teaching, learning, and outreach. College computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of information technology resources, such as recreational activities, non-academic and non-business services.

4.2. Unacceptable System and Network Activities

Unacceptable system and network activities include:

- Engaging in or effecting security breaches or malicious use of network communication including, but not limited to
    - obtaining configuration information about a network or system for which the user does not have administrative responsibility.
    - engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.
- Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.

- Interfering with or denying service to another user on the campus network or using college facilities or networks to interfere with or deny service to persons outside the college.

4.3. Unauthorized Use of Intellectual Property

Users may not use college facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

- Except as provided by fair use principles, engaging in unauthorized copying, distribution, display or publishing of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.
- Using, displaying or publishing licensed trademarks without license or authorization or using them in a manner inconsistent with terms of authorization.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Using computing facilities and networks to engage in academic dishonesty prohibited by college policy (such as unauthorized sharing of academic work, plagiarism).

4.4. Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

- Setting up file sharing in which protected intellectual property is illegally shared.
- Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Inappropriate use or sharing of college-authorized IT privileges or resources.
- Using IT resources for political or religious purposes without authorization from the College president or his/her designee.
- Using IT resources to harass or intimidate another person.
- Changing another user's password, access, or authorizations.
- Using IT resources to actively engage in displaying, procuring or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.
- Using IT resources for personal gain.

4.5. Misuse of E-mail and Communications Activities

Electronic mail (e-mail) and communications are essential in carrying out the activities of the college and to individual communication among users and their correspondents. Individuals are required to know and comply with the college's Mass E-Mail policy. Some key prohibitions include:

- Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, except as approved on the Mass E-Mail policy.
- Engaging in harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.
- Masquerading as someone else by using their e-mail or internet address or electronic signature.

- Soliciting e-mail from any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or solicitations for business schemes.
- Using e-mail originating from within JC's networks for commercial purposes or personal gain.
- Sending the same or similar non-business-related messages to large numbers of e-mail recipients or newsgroups.

5. Reporting Incidents

Alleged incidents involving students should be reported to the Vice President of Enrollment and Student Services.

Alleged incidents involving employees or community partners should be reported to the Vice President of Human Resources and Administration.

Violations of this policy are prohibited and may also be violations of other College policy and in some cases may constitute criminal offenses. Users must report information they have concerning instances in which this policy has been or is being violated.

6. Sanctions

The Responsible Use policy is enforced through the following mechanisms.

6.1 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.

6.2 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.

6.3 Non-represented employees who engage in any activity that violates the Responsible Use Policy are subject to disciplinary action pursuant to College policy.

6.4 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.

Change Log:

Date Of Change	Version	Description of Change	Responsible Party
4/2/13	1.0	Updated Content	J. Jones
07/13/2016	2.0	Biennial Review	J. Jones