JOLIET JUNIOR COLLEGE 1901

BOARD POLICIES

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (1)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

Joliet Junior College reserves the right to amend or otherwise revise this document as necessary to reflect future changes made to its Technology Resources. You are responsible for reviewing this Policy periodically to ensure continued compliance with all Joliet Junior College guidelines.

1.0 Overview

Joliet Junior College provides a technology and information environment to support its educational activities and administrative functions. These Technology Resources, including network and wireless infrastructure, computing systems, software, internal and external data, voice, video, and Internet services, are shared resources which are operated by and are the sole property of the College. To ensure and maintain secure and reliable operations, the College expects all users, including students, faculty, staff, administrators, other employees, contractors, vendors, guests, visitors and members of the general public using the College's Technology Resources, whether on-campus or remotely off-campus, to abide by the JJC Responsible Use Policy, related policies and procedures, and all applicable federal, state, and local laws. Two guiding principles for determining acceptable use for technology are: (1) all the College's Technology Resources exist to support the College's mission, and (2) the College is committed to ensuring a positive learning environment for all members of its community. The College reserves the right to restrict or deny access to its network or other Technology Resources for those who violate the Responsible Use and related policies and procedures. Further, violations may result in disciplinary action, including suspension, dismissal, and/or legal proceedings.

2.0 Definitions

- The term **"College"** means Joliet Junior College and all Technology Resources at satellite sites and Extended Campuses.
- The term **"Technology Resources"** means any College network and wireless infrastructure, computing systems, software, internal and external data, voice, video, and Internet services.
- The term **"Display"** means intentionally bringing up anything visual or auditory for observation.
- The term **"Obscene"** means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude is obscene.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (2)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

- The term **"Threatening"** means communications which result in a reasonable person being disturbed by or fearful of bodily, emotional, or mental harm.
- The term **"Harass"** means to engage in knowing and willful conduct directed at another which a reasonable person would find alarming, upsetting or disturbing. Harass also means to subject another to unwelcome sexual advances, requests for sexual favors, and other verbal, visual or physical conduct of a sexual nature. For further clarification see Board Policy 2.2.2 Sexual Harassment.

3.0 **Policy**

This policy applies to all users, including students, faculty, staff, administrators, other employees, contractors, vendors, guests, visitors and members of the general public who use the College Technology Resources. These individuals are required to take reasonable and necessary measures to safeguard the operating integrity of College-owned or College-leased Technology Resources. Individuals are required to prevent access by unauthorized users while acting to maintain a working environment conducive to carrying out the College's mission of instruction, scholarship, and public service. The College expects that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standards of ethics. The user agrees to hold harmless the College, its employees and agents from any claim arising out of the user's breach of this Policy.

Only authorized users are granted access to Technology Resources, and users are limited to specifically defined, documented and approved applications and levels of access rights. Access control for Technology Resources is achieved minimally via user IDs that are unique to each individual user to provide individual accountability. Any user accessing the College networks and systems must be authenticated. The level of authentication must be appropriate to the data classification and transport medium.

Because of the richness of the Internet and the College's Technology Resources, it is not possible to catalogue exhaustively all acceptable and unacceptable uses. Prior to actual utilization of unfamiliar Technology Resources, employees and students should consult their supervisors or classroom instructors, respectively, about the appropriateness of such uses.

JOLIET JUNIOR COLLEGE 1901

BOARD POLICIES

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (3)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.1 Appropriate Use of Technology

The College's Technology Resources are used to support its teaching, research, service, social, administrative, and union functions. Activities deemed to be appropriate uses of College Technology Resources include but are not limited to the following:

3.1.1 Appropriate Educational Use (students)

Carrying out College course assignments and activities (See Article 8 of the Faculty Contract and Board Policy 7.6.2 Academic Freedom) requiring access to and use of campus Technology Resources, including:

A. Authorized access to and use of computer programs licensed by JJC available on stand-alone and networked College Technology Resources (e.g., workstations, laptops, kiosks).
B. Authorized access to lab and campus networks to perform and complete required course work for College courses in which the student is currently enrolled.
C. User access to authorized College student email accounts.
D. Independent study and research.
E. Agreement by user to follow Responsible Use Procedures established by individual computing labs and Technology Resources and obey directives issued by authorized College personnel supervising such labs and College systems.

3.1.2 Appropriate Instructional Use (faculty)

All College academic settings involving preparation and instruction will follow the current contractual agreement between ICC District 525 and JJC Faculty Council AFT Local 604 regarding academic freedom (See Article 8 of the Faculty Contract and Board Policy 7.6.2 Academic Freedom). The following general uses are accepted:

A. Use in classroom instruction. College-approved software, hardware, and accessories needed by faculty as part of their instruction and research efforts are allowed.
    1. Any downloading or sharing of materials must comply with copyright laws and any software used on College-owned Technology Resources must have a valid license.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (4)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

2. If software is requested to be installed or upgraded on a College computer, it is the software owner's or licensee's responsibility to ensure licensing requirements have been met.

B. Development of instructional materials.
C. Research connected to academic and instructional concerns and interests.
D. Communication related to the business of the College with colleagues, students, institutions, and professional organizations.
E. Accessing Technology Resources after hours and on weekends for teaching, training, and research needs.

3.1.3 **Appropriate Administrative Use (College employees)**

A. Administrative communications, business communications and business transactions.
B. Communication related to the business of the College with colleagues, students, institutions, and professional organizations.
C. Research tied to College concerns and interests.
D. Accessing Technology Resources during lunch and breaks.

3.1.4 **Appropriate Personal Use (College employees)**

(Administration, faculty, and staff)

Employee personal use of College computers and equipment, including Email and Internet access, is an accepted and appropriate benefit of being associated with the College's rich Technology Resource environment. However, all the following conditions, which may be verified by the employee's supervisor, must be met:

A. There is little or no cost to the College.
B. Any use (excluding lunch and breaks) of Technology Resources
    1. does not exceed 3% of an Administrator's work day at the College;
    2. does not exceed 3% of a Staff member's work day at the College;
    3. By Faculty is governed by Article 8 of the Faculty Contract and Board Policy 7.6.2 Academic Freedom.
C. The use does not interfere with the performance of the employee's official duties.
D. The use does not disrupt or distract from the conduct of College business due to volume or frequency.
E. The use does not disrupt other College employees and does not obligate them to make personal use of College resources.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (5)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

F. The use does not compromise the security or integrity of College property, information, or software.
G. The use does not negatively impact the Technology Resources of the College.

3.1.5 Appropriate Guest Use

The College provides guest Internet access for visitors over an unsecured wireless network and on public computers located in designated computer labs and in kiosks. Guests are welcome to use the College's Guest Network as long as their activities do not interfere with those of the campus community.

The guest user agrees to follow Responsible Use Procedures established by individual computing labs and Technology Resources and obey directives issued by authorized College personnel supervising such labs and College systems.

3.2 Inappropriate Use of Technology Resources

Use of College Technology Resources for purposes other than those identified in section 3.1 is not permitted. Users are prohibited from using the College Technology Resources in any manner identified in this section and are not limited to these examples.

Any user who violates this section of the procedure by engaging in inappropriate use of College Technology Resources shall be subject to revocation or suspension of user privileges, student or employee disciplinary procedures, and may be subject to criminal or civil sanctions as defined by law.

3.2.1 Specific Examples of Inappropriate Use

Specific examples of inappropriate use of Technology Resources include, but are not limited to:

A. Accessing unauthorized information.
B. Disrupting colleagues and/or work environment inside or outside of working hours.
C. Violating the rights of others by publishing or displaying any information that a reasonable person might find offensive, obscene, known to be inaccurate or false, profane, or threatening. This does not apply to academic classes and College-approved activities.
D. Using the Technology Resources in a way that interferes with any College activities and obligations.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (6)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

E. Interfering with the security or operation of Technology Resources.
F. Attempting to alter or gain or actually altering or gaining unauthorized access to files or any other Technology Resources.
G. Attempting to or actually damaging, altering, or disrupting the operations of Technology Resource files or systems.
H. Attempting to or actually vandalizing equipment, software, hardware, or data belonging to the College or others.
I. Supporting, promoting, or soliciting for an outside organization or group unless otherwise authorized by law and/or College policy.

3.2.2 **Violations of College Policy**

It is contrary to College policy for a user to use, submit, publish, display, or transmit on the network or on any Technology Resource any information which:

A. Contains material which is defamatory, offensive, harmful, hateful, abusive, obscene, pornographic, profane, threatening, or otherwise biased, discriminatory (based upon protected classes), or illegal.
B. Deliberately inhibits other users from using the system or affects the efficiency of the Technology Resources.
C. Uses Technology Resources for the purpose of criminal intent or any other illegal purpose.
D. Violates or infringes on the rights of any other person, including the right to privacy.

3.2.3 **Other Examples of Unacceptable Use**

It is also unacceptable for a user to use College Technology Resources to:

A. Display, view, download or send pornographic or other obscene materials.
B. Conduct any unauthorized fundraising or public relations activities for non-College entities.
C. Knowingly pass on material, information, or software in violation of College policy and/or federal, state, and local laws.
D. Conduct, promote or advertise unauthorized personal, commercial, or private enterprise (this excludes public speaking on behalf of the College).
E. Advertising and/or selling for personal commercial purposes without prior College authorization.
F. Endanger productivity of College students and employees.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (7)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

G. Bully, harass, or belittle others.

3.3 Electronic Mail (Email)

The College provides electronic mail resources to facilitate communication, student learning, public service, safety, and any College-related task or issue. In particular, students and employees of the College are assigned a College email account and are expected to access their College email regularly in order to receive and respond to important notices and information (e.g. personal and account information, emergency situations, severe weather advisories, school closings and major event cancellations). Authorized College faculty, staff and students are allowed to access their College accounts from any appropriate computer lab, kiosk, or designated computer on any College campus.

When using email, users shall abide by conventional etiquette guidelines developed for the Internet ('Netiquette'). These guidelines can be found by searching the Internet. In addition to Netiquette, users should consider the ethical and/or legal aspects of email correspondence.

3.3.1 Privacy, Confidentiality and Public Records Considerations

The College will make reasonable efforts to maintain the integrity and effective operation of its email systems. Student, faculty, staff and administration email may not be searched without just cause and prior approval from the President of the College. Users are advised that these systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the College can assure neither the privacy of an individual user's use of the College's email resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored on these systems.

A. Users should be aware their College email messages, (including those created, deleted, sent, or received by faculty, staff or administrators in connection with College business) may be considered public records and may be disclosed to members of the public upon request, subject to FOIA, FERPA, and any other legal restrictions.
B. Email is archived at the discretion of the College.

3.3.2 Permissible Use of Electronic Mail

A. Authorized College students, faculty, staff and administration are allowed to use the College's email systems and resources.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (8)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

B. Authorized third-party contractors, vendors, guests, and other persons who have received permission from the Vice President of Learner Support and Technology Services are allowed to use the College's email systems and resources.
C. The use of any College resources for email must be related to College business, including academic pursuit (faculty development, education, seminars, etc.). Incidental and occasional personal use of email, subject to the provisions of responsible use of information technology as set forth in article 3.1.4 of this policy, may occur when such use does not generate a direct cost to the College (e.g., printing email).

3.3.3 **Best Practices**

Authorized College faculty, staff and students shall

A. ensure that messages are addressed to the appropriate recipient(s).
B. not subscribe to list servers or other distribution lists that are not College related. Such lists tend to overload and affect the performance of the email system
C. not compromise password confidentiality by giving passwords to others or exposing passwords to public view.
D. change passwords on a regular basis.
E. retain messages only if relevant to the work or any pending litigation. The College's email system will retain messages according to the College Email policy. Messages having a legitimate business purpose should be archived or printed and filed.
F. address messages to recipients who "need to know." Messages sent unnecessarily to a long list of recipients' lowers system performance, and may annoy recipients.
G. avoid opening messages or attachments received from unidentifiable senders. Messages and attachments can carry viruses and other malicious content.
H. construct messages professionally and completely.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (9)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.3.4 **Prohibited Use of Electronic Mail**

The following use of email is strictly prohibited. Employees aware of any violation should immediately report the violation to their supervisor or Human Resources representative. Students should contact their instructor or the Dean of Students.

A. Unauthorized use (e.g., accessing someone else's email), forging or fraudulently modifying email, or distorting the meaning of the original email text.
B. Knowingly or recklessly sending unsolicited mail or messages (mass mailing). Examples of such broadcasts include chain letters, advertisements, solicitations, viruses, hoaxes, spam mail, and other email schemes that may cause excessive network traffic or bandwidth use (see Broadcast Email section 3.3.5).
C. Attempting to breach any security measures on any email system, or attempting to intercept any email transmissions without proper authorization.
D. The creation and/or exchange of messages that, to a reasonable person, would be considered offensive, harassing, obscene or threatening.
E. The exchange of privileged, confidential or sensitive information to inappropriate persons.
F. Sending messages from another person's account.

3.3.5 **Broadcast Email**

Those who anticipate sending electronic mail messages to the entire master list of employees and/or students for official College or academic purposes are responsible for consulting with their supervisor, Vice President or Communications and External Relations to determine the appropriate means for distributing messages with the least impact on campus network and computing resources.

Authority to use the entire master list of email addresses of College employees rests with the Senior Staff.

Authority to send email to all students rests with the College President, Vice-Presidents, Communications and External Relations, Deans, Director of Student Activities and Campus Police.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (10)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.4 Administrative Systems Access

College employees will be given access to the College's administrative systems as needed. Accounts and security clearance must be authorized by a Director or Vice-President.

3.5 Internet

The Internet provides a means of accessing information useful for students, employees, and guests of the College. Users should abide by conventional etiquette guidelines developed for the Internet ('Netiquette'). These guidelines can be found by searching the Internet.

3.5.1 Internet Appropriate Use

Users are responsible for making sure they use this access correctly and wisely. Acceptable uses include but are not limited to:

A. Access to and sharing of information that is in direct support of College students and/or College-related business.
B. Communication of information related to student or professional development.
C. Keeping current on topics of general College interest.
D. Encouraging collaboration and sharing of resources.

3.5.2 Internet Inappropriate Use

Unacceptable uses include but are not limited to:

A. Intentionally viewing, downloading or distributing anything that a reasonable person might find offensive, obscene, profane, or threatening.
B. Compromising productivity of the College.
C. Violating federal, state, and local laws.
D. Distributing or printing copyrighted materials found on the Internet.

3.6 Network Use and User Accounts Guidelines

The primary purpose of the College's network is to serve members of the campus community – JJC students, faculty, staff, and guests. Use of the College's Network, Internet connection and email resources is a privilege and it is expected that all users given access abide by the Responsible Use guidelines. The College reserves the right to extend, restrict, or deny privileges and access to its Technology Resources.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (11)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.6.1 **Network Appropriate Use**

College facilities and accounts are to be used for the activities or purposes for which they are designated. Appropriate uses of network and user-accounts include:

A. Accessing only those computer accounts for whose use they have been authorized. Users must identify computing work with their own username or other approved IDs so that responsibility for the work and/or student activity can be identified.
B. Using accounts for authorized purposes. This policy shall not prevent informal communication.
C. The maintaining, by Network administrators, general files and communications as a whole to ensure system integrity.
D. Maximizing the use of technologies covered under this user policy to reduce the cost of postage, letters, reports, etc.

3.6.2 **Network Inappropriate Use**

Inappropriate uses of network and user-accounts include:

A. Establishing a major network service, introducing a service that conflicts with a centrally, predefined service, or obtaining network connectivity without coordinated planning and prior approval from the Vice President of Learner Support and Technology Services.
    1. This need for planning and prior approval also extends to, but is not limited to, network wiring, network infrastructure, dial-up service, network addresses and naming conventions, network-attached computer labs, and wireless access points.
B. Knowingly or recklessly downloading, distributing, or streaming data (text, audio, video…) files large enough to disrupt or compromise Network Resources. The College reserves the right to take any steps necessary to preserve the integrity and stability of the Network Resources.
C. Breaching the security of Technology Resources and Systems through the use of **LOOPHOLES**, system deficiencies, knowledge of computer or network security systems, or knowledge of a password to do any of the following, including, but not limited to, damaging a computer or computers, compromising network systems, obtaining extra resources, taking resources from another user or gaining access or attempting to

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (12)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

gain access to restricted resources for which proper authorization has not been given.

D. Providing access to others through their College network connection.
   1. All users accept full responsibility for all violations that occur while they are logged on to the College network. When users leave a workstation, they are expected to properly lock or log out of all applications and networks.

E. Accessing network infrastructure devices without proper authority.
   1. A notice will be displayed, where applicable, warning that only those with proper authorization are allowed to access the system. A warning message will make clear that the system is a private network or application and unauthorized users should disconnect or log off immediately.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (13)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.6.3 **Need-to-Know**

Users will be granted access to information on a "need-to-know" basis based on their user account role at the College. That is, users will only receive access to the minimum applications and privileges required to carry out their responsibilities.

3.6.4 **Employee Compliance Statements**

College employees and students must sign a compliance statement regarding the use of Technology Resources prior to receiving a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by College policies and procedures related to Technology Resources.

3.6.5 **Third-Party Access (Non-Employee)**

Contractors, consultants, business partners, or individuals who are not employees or students will be allowed to access the College's Guest Network, but they will not be granted a user-ID or be given additional privileges to use College Technology Resources unless they have obtained written approval from the VP of Learner Support and Technology Services.

3.6.6 **Remote Access**

Remote access must conform to all federal, state, and local statutory requirements including but not limited to the Family Educational Rights and Privacy Act (FERPA).

3.6.7 **Accountability**

Users shall not disclose their login and password to anyone. Authorized users are responsible for the security of their passwords and accounts. Passwords shall be changed according to College policy.

3.7 **Intellectual Property**

All members of the College community must observe the College's intellectual property rights.

3.8 **Copyright**

Copyright laws do not allow a person to store, distribute, or alter the content of copyrighted material unless permission has been granted by the copyright holder. Each user is responsible for observing all federal copyright laws. Users must honor copyright laws regarding protected commercial software used at the College. For exceptions to copyright law related to academic use, contact the reference librarians in the college Learning Resource Center (LRC).

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (14)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

3.8.1 **Fair Use**

The academic community will follow "reasonable and good-faith" attempts to apply fair use to meet their educational objectives based on the fair use provision of copyright law, Section 107 of the Copyright Act of 1976. "Notwithstanding the provisions of sections 106 and 106A (Title 17 of the United States Code), the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. If a user makes a request for, or later uses copyrighted work for purposes in excess of "fair use," that user may be liable for copyright infringement."

3.8.2 **Software Compliance with Copyright Laws**

All employees and students who use software owned or licensed by the College must abide by all terms and conditions of the software license agreement(s).

3.9 **Security**

Attempts, successful or unsuccessful, to alter system software, to bypass security protocols, to introduce viruses, worms, or other malicious or destructive programs, or otherwise "to hack" are expressly forbidden. Anyone who attempts to breach or breaches security will be prosecuted or disciplined to the fullest extent of the law and/or College policy.

3.9.1 **Prohibited Use**

No one may compromise the security of Technology Resources and Systems through the use of loopholes, system deficiencies, knowledge of computer or network security systems, or knowledge of a password to attempt or actually to do any of the following, including, but not limited to, damaging a computer or computers, compromising network systems, obtaining extra resources, taking resources from another user or gaining access or attempting to gain access to restricted resources for which proper authorization has not been given.

3.9.2 **System Access Controls**

Active workstations should not be left unattended for prolonged periods of time; where appropriate users should lock down their workstations/laptops. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on.

3.9.3 **Logs**

All inbound and outbound access of the College's internal network must be maintained. Audit trails for confidential systems should be backed up and stored in accordance with the College back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot be viewed by unauthorized persons. All logs must be audited on a periodic basis.

3.10 **Privacy of Information**

The College respects the privacy of individuals' electronic files and will take reasonable steps to protect that privacy. Moreover, it is the expectation of the College that individual members of the electronic community have an obligation to show the same respect for the privacy of the other members of the community. Users should understand, however, the limited privacy afforded by electronic data storage and electronic mail and should apply appropriate security to protect private and confidential information. To this end, the College reserves the right to access its Technology Resources at any time.

3.10.1 **Expectations**

A. Members of the College community are expected to be knowledgeable of the provisions of:
   1. FERPA - Family Educational Rights and Privacy Act designed to protect the confidentiality of data and the privacy of individuals (http://www.ed.gov/policy/gen/reg/ferpa/index.html).
   2. PIPA – Personal Information Protection Act requires that any entity that collects and maintains personal consumer information must notify all affected Illinois customers in the event of a security breach (http://www.ilga.gov/LEGISLATION/ILCS/ilcs3.asp?ActID=2702).
   3. FOIA – The Freedom of Information Act provides that any person has the right to request access to public records or information. Valid legal requests for information include but are not limited to

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (16)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

subpoenas, litigation or potential litigation, violation of federal or state law or College policy, and an Illinois FOIA request may allow inspection of electronically stored information. In many instances, electronic files are treated in the same way as paper files. For instance, FOIA allows inspection of public documents (including electronic files), as defined by FOIA, through an appropriate FOIA request. This means that every electronic file is subject to inspection unless there is a specific legal reason that such material is protected (http://www.ag.state.il.us/government/foia_illinois.html).

B. Employees who access College information that is needed in the performance of their normal duties must exercise good judgment and professionalism in the use of such information. In particular, confidential identifying information or demographic data, which pertains to students, employees, or College operations, must be used in a manner that protects rights of privacy and limits personal and institutional liability.
C. Students are prohibited from accessing confidential College information about anyone except themselves. This prohibition does not imply that students have complete access to confidential information about themselves except information covered under FOIA.
D. Users of College Technology Resources are subject to all College policies and procedures, and all applicable federal, state, and local laws related to privacy of information.

4.0 **Internet Service Provider Policy Guidelines**

The College is bound contractually to the guidelines given in Acceptable Use Policies of its Internet provider(s) in regard to electronic traffic originating from the College.

5.0 **Enforcement and Penalties**

Individuals or groups who act in a manner contrary to existing policy for acceptable use or who take actions which have legal implications are subject to appropriate sanctions. The College reserves the right, at all times, to suspend or revoke the privilege of access to College Technology Resources. Violations of this policy shall be cause for disciplinary review. Alleged violations of this policy shall be subject to, but, not limited to the procedures outlined in the College Board Policies, College collective bargaining agreements, Employee Full and Part-time Handbooks, Student Worker Handbook, Student Handbook, and the Student Code of Conduct.

DIVISION	REFERENCE NO.
X. Information Technology	10.1 (17)
CATEGORY	**DATE**
10.1 Responsible Use of Information Technology	Adopted 11/95 Revised 5/06, 12/09

Penalties for non-compliance may include but are not limited to:

- Suspension or usage restrictions of Internet service and E-mail/messaging services.
- Internal disciplinary measures, including discharge.
- Initiation of criminal or civil action, if appropriate**.**