Responsible Use of Information Technologies at Springfield College

The Springfield College Responsible Use of Information Technology Policy is to serve as a guideline by which faculty, staff, and students can review the requirements of ethical and legal behavior within the College community when using electronic computing devices and resources, network or the Internet.

The College provides the campus community with technology resources for the purposes of teaching, learning, scholarly research, and administrative tasks. Available resources include, but are not limited to, software, hardware (including but not limited to telephones, computers, laptops, iPads, and media equipment) either owned or leased by the College. This policy applies both to users of College equipment and to owners of personal equipment that is connected to the data or telecommunications infrastructure of the College.

Access to and use of computing and networking resources at Springfield College are privileges extended to members of the Springfield College community. The use of College computing resources, like any other College-related activity, is subject to the normal requirements of legal and ethical behavior within the College community. Members of the Springfield College community may use these resources for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the College, and other College-sanctioned or authorized activities. The use of technology resources provided by the College for purposes other than teaching, learning, scholarly research, and the institutions administrative functions may be terminated if it interferes in any way with those primary endeavors.

Springfield College acknowledges that occasionally students and faculty and staff members use College resources assigned to them or to which they are granted access for noncommercial, personal use. Such occasional noncommercial uses are permitted by faculty, staff, and students if they are not excessive; do not interfere with the performance of any faculty member, staff member, or student's duties; do not interfere with the efficient operation of the College or its computing resources; and not otherwise prohibited by this policy or any other College policy or directive.

Because computing systems have such great power, activities that might at first seem to be merely mischievous can harm an entire College community and beyond. Any unauthorized access or interference with system functionality is unacceptable. College-wide guidelines such as the **Student Handbook, Discrimination/Harassment Policy, and Copyright Policy** apply to the use of computing resources, as do community standards of consideration for others, and the mission of the College. Federal, state, and local laws and regulations also apply.

Springfield College computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purposes that is illegal,

immoral, unethical, dishonest, damaging to the reputation of the College, inconsistent with the mission of the College, or likely to subject the College to liability. Impermissible uses (some of which may constitute illegal uses) include, but are not limited to, the following:

- Harassment
- Libel or slander
- Fraud or misrepresentation
- Destruction of or damage to equipment, software, or data belonging to the College or others
- Disruption or unauthorized monitoring of electronic communications
- Unauthorized copying or transmission of copyright-protected material
- Use of the College's trademarks, logo, insignia, or copyrights without prior approval
- Violation of computer system security
- Unauthorized use of computer accounts, access codes (including passwords) or network identification numbers (including email addresses) assigned to others
- Use of computer communications facilities in ways that unnecessarily impede the computing activities of others
- Development or use of unapproved mailing lists
- Use of computer facilities for private business purposes unrelated to the mission of the College or to College life
- Academic dishonesty
- Violation of software license agreements
- Violation of network usage policies and regulations
- Violation of privacy
- Viewing, posting or sending obscene, pornographic, sexually explicit, or offensive material
- Posting or sending material that is contrary to the mission and values of the College
- Intentional or negligent distribution of computer viruses

Responsibilities of Users
The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Computer accounts, passwords, and other types of authorization should not be shared with others
- Understand the level or protection the computer systems automatically apply to files and supplement if necessary, for sensitive or confidential information
- Be aware of computer viruses and other destructive computer programs, and take steps to avoid them
- Understand that the user has ultimate responsibility for resolution of problems related to the invasion of the user's privacy or loss of data
- Be sure to make backup copies of all important data
- Respect the privacy of others

- Be sure to comply with all federal, state and other applicable laws as well as College policies and regulations
- Change passwords on a regular basis

Software Ethics Policy

Springfield College prohibits the illegal use of software on campus. Springfield College may apply sanctions to those who engage in the following actions:

- Configuring the software and making modifications
- Designed to fit the software to the user's needs
- Selling or giving the original copy and documentation to another
- Providing copies of copyrighted or licensed software to others while maintaining copies for one's own use, unless there is a specific provision in the license allowing such activity.
- Using software or documentation knowingly obtained in violation of the copyright law or a valid license provision. Use of a copy of a copyrighted program obtained from another party where no license permits such reproduction or transfer will be presumed to be a knowing violation of copyright or license provisions. The burden of demonstrating that the use was innocent will rest with user.
- Using a copyrighted program on more than one machine at the same time unless a specific license provision permits such activity.

The following actions are considered illegal. Springfield College may apply sanctions to those who engage in these actions.

- Providing copies of copyrighted or licensed software to others while maintaining copies for one's own use, unless there is a specific provision in the license allowing such activity.
- Using software or documentation knowingly obtained in violation of the copyright law or a valid license provision. Use of a copy of a copyrighted program obtained from another party where no license permits such reproduction or transfer will be presumed to be a knowing violation of copyright or license provisions. The burden of demonstrating that the use was innocent will rest with user.
- Using a copyrighted program on more than one machine at the same time unless a specific license provision permits such activity.

Security

Springfield College will assume that users are aware that electronic files are not necessarily secure. Users of electronic mail systems should be aware that electronic mail is generally not secured and is extremely vulnerable to unauthorized access and modification. The Office of Internet Technology Solutions (ITS) will make available to interested persons information concerning reasonable methods for attempting to protect information on central computing systems from loss, tampering, unauthorized search, or other access.

Privacy and Confidentiality

Springfield College reserves the right to inspect and examine any Springfield College owned or operated communications system, computing resource, and/or files or information contained therein at any time.

Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. In general, the College information stored on computers is confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on College-owned equipment. Additionally, the College may access email and data stored on Springfield College's network of computers for the following purposes:

- Troubleshooting hardware or software problems
- Preventing unauthorized access and system misuse
- Retrieving business related information*
- Investigating reports of violation of College policy or local, state, or federal law*
- Complying with legal requests for information*
- Rerouting or disposing of undeliverable mail

*The system administrator will need specific approval from the Office of Human Resources or the appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.

Reporting violations
All users should report any discovered unauthorized access attempts or other improper usage of Springfield College computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem, with any College computer or network facilities, including violations of this policy, you should notify the chief information officer, the Office of Human Resources, or other appropriate administrator.

Sanctions
Violations of this policy will be treated as violation of College policy and/or violations of civil or criminal law. The Office of ITS in conjunction with the Office of Human Resources will investigate apparent or alleged violations of these guidelines. The College reserves the right to immediately suspend user privileges pending investigation. Such action will be taken to protect the security and integrity of the computer system and will take precedence over its impact on the individual's work.

When appropriate, at the discretion of the director of human resources and the chief information officer, cases of apparent abuse will be reported to the vice president for student affairs (student cases), the vice president for academic affairs (faculty cases), or the director of human resources (staff cases). These offices are responsible for determining any further disciplinary action. Upon a finding of a violation, disciplinary measures may include warnings, suspension of user privileges (temporary or permanent), disciplinary action up to and including termination of employment. The College also may pursue civil and/or criminal charges if it deems appropriate.

Questions regarding this policy should be sent to:
Chief Information Officer, ext. 3532 or
Director of Human Resources, ext 3118