Acceptable Use Policy

Electronic Communications Policy

Effective Date: March 1, 2009
Revised: March 3, 2009
Status: 

Responsible University Officer: Vice President, Information Technology
Responsible Coordinating Office: Office of Information Technology

Version 1.0

PURPOSE

To remain competitive, better service our customers, and give our talented workforce the best tools to do their jobs, Cardinal Stritch University continues to adopt and make use of new means of communication and information exchange. This means that many of our Employees have access to one or more forms of electronic media and services, including computers, e-mail, telephones, University provided cell phones, voice mail, fax machines, external electronic bulletin boards, wire services, on-line services, the Internet, and the World Wide Web.

Cardinal Stritch University encourages the use of these media and associated services to enable more efficient and effective communication and to have valuable sources of information about vendors, customers, technology, and new products and services. However, all Employees and everyone connected with the University should remember that electronic media and services provided by the University are Cardinal Stritch University property and their purpose is to facilitate and support University business.

This policy cannot establish rules to cover every possible situation. Instead, it is designed to express the University’s philosophy and set forth general principles Employees should apply when using electronic media and services.

The following procedures apply to all electronic media and services that are:

- Accessed on or from any University site, including all satellite locations;
- Accessed using University computer equipment or via University-paid access methods; or
- Used in a manner that identifies the individual with the University.

PERSONAL USE

Cardinal Stritch University provides electronic media and services primarily for Employee’s business use. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-
Acceptable Use Policy

Cardinal Stritch University allows incidental personal use of its electronic media and services subject to the following conditions and restrictions during work hours:

a. Personal use must be infrequent and must not:
   • Involve any prohibited activity;
   • Interfere with the productivity of the Employee or his or her co-workers;
   • Consume system resources or storage capacity on an ongoing basis, or
   • Involve large file transfers or otherwise deplete system resources available for University business purposes.

b. Using electronic media and services to participate in any newsgroup, mailing list, bulletin board, or other type of discussion forum that is not job related is not incidental use and is strictly prohibited.

c. Employees should not have any expectations of privacy with respect to personal e-mail sent or received on Cardinal Stritch University’s e-mail system. Employees should delete personal messages as soon as they are read or replied to. Employees should not store copies of the personal messages they have sent. Because e-mail is not private, Employees should avoid sending personal messages that are sensitive, confidential, or containing any questionable content.

PROHIBITED ACTIVITIES

Employees are strictly prohibited from using any of the University electronic media and services in connection with any of the following activities:

• Engaging in illegal, fraudulent, or malicious activities;
• Engaging in activities on behalf of organizations with no professional or business affiliation with Cardinal Stritch University (for example, University resources, including email, are not to be used for home based businesses such as Avon, Pampered Chef or Stanley Products)
• Sending or storing offensive, obscene, or defamatory material;
• Annoying or harassing other individuals;
• Sending uninvited e-mail of a personal nature;
• Using another individual’s account or identity without explicit authorization;
• Attempting to test, circumvent, or defeat security or auditing systems without prior authorization;
• Permitting any unauthorized individual to access Cardinal Stritch University’s electronic media systems, or
• Distributing or storing chain letters, jokes, solicitations or offers to buy or sell goods, or other non-business material of a trivial or frivolous nature.
ACCEPTABLE USE POLICY

ACCESS TO EMPLOYEE COMMUNICATIONS

Electronic information created and/or communicated by an Employee using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, Internet and bulletin board system access, and similar electronic media generally is not monitored by the University. We respect our Employees’ desire to work without us looking over their shoulder. However, the following condition should be noted:

Employees should not have any expectation of privacy with respect to messages or files sent, received, or stored on Cardinal Stritch University’s electronic media systems. E-mail messages and files, like other types of correspondence and Cardinal Stritch University documents, can be accessed and read by authorized Employees or authorized individuals outside the University. Authorized access to Employee correspondence by other Employees or outside individuals includes, but is not limited to, the following:

a. Access by the system administration staff during the course of system maintenance or administration;

b. Access approved by the Employee, the Employee’s supervisor, or officer of Cardinal Stritch University when there is an urgent business reason to access the Employee’s communications - for example, if an Employee is absent from the office and the supervisor has reason to believe that information relevant to the day’s business is located in the Employee’s e-mail inbox, voice mail, etc.

c. Access approved by the Employee’s supervisor, Cardinal Stritch University’s Human Resources Department, or officer of Cardinal Stritch University when there is reason to believe the Employee is using electronic media and services in violation of Cardinal Stritch University’s policies;

d. Access approved by an officer of Cardinal Stritch University or Cardinal Stritch University’s Human Resources Department or in response to Cardinal Stritch University’s receipt of a court order or request from law enforcement officials for disclosure of an Employee’s communications or files.

Electronic media and services should not be used to communicate sensitive or confidential information. Employees should anticipate that such communications might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals. In addition, while Cardinal Stritch University endeavors to maintain the reliability of its electronic media

---

1 “Sensitive or confidential information” is defined as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.
Acceptable Use Policy

systems, Employees should be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosures of electronic communications.

SECURITY/APPROPRIATE USE

Employees must respect the confidentiality of other individuals’ electronic communications. Except in cases in which explicit authorization has been granted by University management, Employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other Employees or third parties;
- Hacking or obtaining access to systems or accounts they are not authorized to use;
- Using other people’s log-ins or passwords; and
- Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic access to other companies’ or individuals’ materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

PASSWORDS

Each user accesses the University supported e-mail system by means of a log-in name and password.

a. Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. From a systems perspective and from the perspective of an e-mail recipient, passwords also establish the identity of the person sending an e-mail message. The failure to keep passwords confidential can allow unauthorized individuals to read, modify, or delete e-mail messages, circulate e-mail forgeries; and download or manipulate files on other systems.

b. The practice of using passwords should not lead Employees to expect privacy with respect to messages sent or received (see Access to Employee Communications)

c. Employees must choose new passwords every six months. Passwords will be a minimum of 8 characters, a combination of letters, numbers and symbols and should never consist of a proper name or a common word. Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.
Acceptable Use Policy

d. Employees are prohibited from disclosing their password, or those of any other Employee, to anyone who is not an Employee of Cardinal Stritch University. Employees also should not disclose their password to other Employees, except when required by an urgent business matter. Employees should change their password as soon as possible after the urgent business matter has been resolved.

E-MAIL STORAGE POLICY

Cardinal Stritch University strongly discourages the storage of a large number of e-mail messages. Retention of messages takes up a large amount of space on the mail server and can impact system performance. In addition, because e-mail messages can contain Cardinal Stritch University’s confidential information, it is desirable to limit the number, distribution, and availability of such messages.

a. Deletion by Users As a general rule, if a message does not require a specific action or response, it should be deleted after it is read. If the content of the message needs to be saved for more than two weeks, it should be archived to a local hard disk or diskette or printed out and saved to an appropriate file. Employees should review their messages weekly and delete those that are not needed.

b. Deletion by System Administrator Deletion of e-mail messages by the system administrator will be performed on a case by case basis, when the need arises, to maintain system integrity.

ENCRYPTION

Encrypting messages or documents sent, stored or received on Cardinal Stritch University’s systems is encouraged when it further protects the privacy of sensitive and confidential information. However, employees are prohibited from using or installing any encryption software without permission from Cardinal Stritch University’s Office of Information Technology. Employees with a business need to encrypt messages should submit a written request to the Office of Information Technology with a copy sent to their supervisor. Employees who use encryption on files stored on a University computer must provide the Office of Information Technology with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

PARTICIPATION IN ON-LINE FORUMS

Employees should remember that any messages or information sent on Cardinal Stritch University provided facilities to one or more individuals via an electronic network—for example, Internet mailing lists, bulletin boards, and on-line services—are identifiable and attributable to Cardinal Stritch University.
Acceptable Use Policy

Cardinal Stritch University recognizes that participation in some forums might be important to the performance of an Employee’s job. For instance, an Employee might find the answer to a technical problem by consulting members of a newsgroup devoted to the technical area.

Employees should include the following disclaimer in all of their postings to public forums:

“The views, opinions, and judgments expressed in this message are solely those of the author. The message contents have not been reviewed or approved by Cardinal Stritch University.”

Employees should note that even with a disclaimer a connection with Cardinal Stritch University exists and a statement could be imputed legally to Cardinal Stritch University. Therefore, employees should not rely on disclaimers as a way of insulating Cardinal Stritch University from the comments and opinions they contribute to forums. Instead, employees must limit their discussion to matters of fact and avoid expressing opinions while using Cardinal Stritch University systems or a Cardinal Stritch University provided account. Communications must not reveal information about Cardinal Stritch University processes, techniques, trade secrets, or confidential information and must not otherwise violate this or other Cardinal Stritch University policies.

CONFIDENTIAL INFORMATION

All Employees are expected and required to protect Cardinal Stritch University’s confidential information. Cardinal Stritch University’s confidential information should never be transmitted or forwarded to outside individuals or companies not authorized to receive the information. Employees must exercise greater care when transmitting Cardinal Stritch University confidential information using e-mail than with other communication means because e-mail makes it easier to redistribute or misdirect confidential information to unauthorized individuals.

Cardinal Stritch University also requires its Employees to use electronic media and services in a way that respects the confidential and proprietary information of others. Employees are prohibited from copying or distributing copyrighted material - for example, software, database files, documentation, or articles - using the electronic media systems.

CELL PHONES

While the University has moved away from generally issuing cell phones, there are limited employees that must use cell phones to conduct their assigned tasks. Be aware the University does not permit the use of cell phones to conduct business while an employee is operating a motor vehicle, unless the employee

---

2 “Sensitive or confidential information” is defined as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.
Acceptable Use Policy

has safely pulled out of traffic and has turned off the vehicle or placed it into park. Further cell phone conversations are not secure, private conversations and employees should not transmit confidential University information in a public setting.

POLICY VIOLATIONS

Employees who abuse the privilege of University-facilitated access to electronic media or services are subject to corrective action and risk having the privilege removed for themselves and possibly other employees. Employees violating the Electronic Communications Policy are subject to discipline, up to and including termination. Employees using electronic media and services for defamatory, illegal, or fraudulent purposes and Employees who break into unauthorized areas of Cardinal Stritch University's computer system also are subject to civil liability and criminal prosecution.

All University employees are responsible for reviewing and adhering to the published computer related policies found on the web <http://www.stritch.edu/oit>.