Introduction

Computer information systems and networks are an integral part of Rosemont College. The College has made a substantial investment in human and financial resources to create these systems. The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of Rosemont College.

Violations

Violations may result in disciplinary action, which may include termination of employment, in accordance with College policy. Failure to observe these guidelines may result in disciplinary action by the College depending upon the type and severity of the violation, whether it causes any liability or loss to the College, and/or the presence of any repeated violation(s).

Administration

The Vice President for Finance and Administration, reporting to the President of the College, is responsible for the administration of this policy.

Contents

The topics covered in this document include:

Acceptable Use of Technology at Rosemont College

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Supervisor responsibilities

Supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

Information Services responsibilities

The Information Services staff must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

Rosemont College provides access to computing and information resources to support teaching, learning, and the business of the college. All members of the college community who use the college's computing and information resources must do so responsibly. It is the policy of Rosemont College that all members of its community act in accordance with these responsibilities, relevant laws, and in the highest standard of ethics.
Any use that would impede teaching and learning, hinder the functioning and business of the College, violate an applicable license or contract, or damage community relations or relations with institutions with whom we share responsibility, is a violation of this policy.
Violation of this policy may result in suspension of privileges to access the information technology involved, initiation of College disciplinary procedures, which may include termination of employment, or in extreme cases, criminal prosecution under federal or state law.
Computing facilities and accounts are owned by the College and are to be used for the College-related activities for which they are assigned. College computing facilities include the hardware and the software throughout the campus, and the network access to these facilities. The College reserves the rights to limit, restrict, or extend computing privileges and access to its computing resources.
By adopting this policy, the College recognizes that all members of the community are also bound by local, state, and federal laws relating to copyright, security, and their statutes existing and future regarding electronic media.
The College characterizes misuse of computing and information resources and privileges as unethical and unacceptable, and as just cause for taking disciplinary action. This behavior includes, but is not restricted to:

- Use of the computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.
- Unauthorized modification of computer resources or equipment.
- Unauthorized access to computers, software, data, or networks, regardless of whether the computers, software, data or networks are owned by the college. This includes using college computer resources for unauthorized access to networks or data at remote sites.
- Circumventing or attempting to circumvent normal resource limits, login procedures, and security regulations.
- Sending fraudulent or harassing computer mail.
- Employees are prohibited from sending or posting messages that contain abusive or objectionable language, that defame or libel others, or that infringe the privacy rights of others.
- Employees shall not view, download, copy, send, post or access information that is illegal, obscene or otherwise inconsistent with the College’s non-discrimination and non-harassment policies (e.g., sexual images, sexist comments, racist messages, ethnic slurs, religious slurs).
- Breaking into another user's electronic mailbox, or reading someone else's electronic mail without her or his permission.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

Disciplinary action may include the loss of computing privileges and other disciplinary sanctions up to and including non-reappointment, discharge, dismissal, and legal action. In some cases, an abuser of the College's computing resources may also be liable for civil or criminal prosecution.

Internet Access

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. Rosemont College Faculty, Staff, Administrators and Students access the Internet through the College’s internal network.

Policy

The use of the Rosemont College Network to access the Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of these privileges, as well as disciplinary action, which may include termination of employment, as specified in the employee

handbook. Rosemont College Information Services has the authority to determine appropriate use and may deny, evoke, suspend or close any employee's access at any time based upon its determination of inappropriate use by that employee.

Monitoring
Rosemont College reserves the right to review any material accessed by employees with Internet access to determine the appropriateness of such material. Rosemont College may review this material at any time.

Security
Security of Rosemont College computing resources is a high priority, especially since the systems are used for our daily business. Users must abide by the following security steps:

- Do not download software from the Internet onto any disk drive in use at the College without prior consent of Information Services.
- Do not allow any other employee to use your login name and/or password.
- Discovery of any security problem will be reported to your Supervisor and Information Services staff immediately.

Confidential information
The work that Rosemont College conducts includes access to an Administrative Database. The confidentiality of the records contained in this Database is governed by the federal Family Education Rights and Privacy Act of 1974. All information is considered confidential, and communication of this information is restricted to authorized parties in accordance with the provisions of FERPA. The appropriate administrative officer of the College must approve requests for disclosure of this information.

Email Policy

All students, staff, facilitators, faculty, and administrators are given a Rosemont e-mail account. Rosemont's e-mail client is Outlook. Exceptions are made if a specific e-mail client is needed, i.e. Eudora.

- New staff, facilitators, faculty, and administrators will receive a Rosemont e-mail account when:
  1. All necessary paperwork has been received by Human Resources;
  2. The employee has actually commenced employment;
  3. Jenzabar information is forwarded to the Postmaster who will notify the new employee with his/her user name and password.
- New students will receive a Rosemont e-mail account when the Postmaster receives the required information from each of the schools (UC, SGPS). They will be notified of their user name and password via an email message from the Postmaster.
- All will be added to the appropriate list, i.e. staff, administrators, faculty, class of, etc. Mailing lists under rosemont.edu are for the transmission of college-related information only.
- Accounts at 70% quota or higher will be investigated and users will be notified. When the account reaches 100% quota, e-mail will no longer function
- If you receive a virus-related warning, especially one that offers a solution like deleting Windows files:
  1. Do not broadcast the warning.
  2. Verify that it is real and not a hoax by visiting http://hoaxbusters.ciac.org or http://www.symantec.com under Security Response.
  3. Notify the Information Technology Help Line at extension 4357.
- All must agree to the Acceptable Use Policy. Anyone abusing the Acceptable Use Policy will be subject to disciplinary action.

Upon separation from Rosemont College employment, employees' e-mail privileges will be terminated. Students may opt to participate in the Rosemont College Alumnae email service.

- When an employee/faculty member resigns or retires from his/her position, Human Resources will notify the Postmaster who will set a termination date for their e-mail with the exception of Faculty Emeritus who may retain their rosemont.edu account unless they request to no longer use it. This date will be relayed to the employee via e-mail so they can save e-mail messages they wish to take with them. Upon determination of the Dean of each school, Human Resources will be notified of all adjunct faculty/facilitators not returning to the College, HR will notify the Postmaster. The adjunct/facilitator will be notified via e-mail that his/her e-mail privileges will be terminated; if the adjunct returns to the College after this period, the e-mail will be reinstated.
- When an employee is terminated from his/her position, Human Resources will notify the Postmaster who will stop their e-mail account and delete contents on the date indicated by Human Resources.
- Graduating students will be notified about the status of their Rosemont e-mail account and given the option to participate in the Rosemont College Alumnae email service. Accounts at 70% quota or higher and/or inactive for a year will be eliminated.

E-Mail Procedures

Attachments: If you must deal with attachments, make sure you have a verbal communication with the other party or parties. If you receive an attachment, even if it is from someone you know, verify that they indeed sent you an attachment. Then, download it, or save it to your computer. Usually the right button of your mouse will give you the opportunity to "Save As". Then go find the document, right click it again, and you can scan that document for viruses for added security. If you send a document, tell the person to expect it before you send it. This also applies to "links" included in e-mail. Do not click any link unless you are absolutely sure that you know who sent it, and where the link will take you.

Deleting Mail: Delete mail or empty your trashcan on a regular basis. Mail stored in the trash does not compact therefore it uses more of your disc space. If the trash can/deleted mail folder is too full, e-mail will not function. If you do not know what to do with the e-mail and don't want to delete, make a folder and move it to the folder. When mail is deleted and the trash emptied, the folders on your desktop compact.

Remote Access

To check e-mail remotely, or from a computer other than your day-to-day computer, you may do so via the web at http://owa.rosemont.edu.

Things to Remember:

- Rosemont's web-based e-mail program is limited in scope and is not recommended for reading and archiving large amounts of e-mails, or for sending large attachments, such as graphic files. Large files can be compressed using a zip utility before being attached.
- Those receiving numerous e-mail messages should forward their rosemont.edu mail to another web-based e-mail system, or use a local e-mail management system.
- The size of your Rosemont account mailbox is limited. You should check your mail often and delete old messages or store them on your hard drive or diskette. You should always try to maintain a quota of 50% or less.
- Do not leave important or essential e-mail on the Rosemont server. It is possible for an account to become inaccessible, necessitating it being deleted and re-created. In this case, e-mail and address books will be lost.

Downloads

Software downloads from the Internet are not permitted unless specifically authorized in writing by the Office of Information Services.

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Rosemont College policies dealing with security and confidentiality of company records.
5. Run a virus scan on any file(s) received through the Internet.
6. Avoid transmission of nonpublic customer information, such as Social Security number, or credit card information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action, which may include termination of employment, by the company and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the College and *may be regarded as public information*. Rosemont College reserves the right to access the contents of any messages sent over its facilities if the College believes, in its sole judgment, that it has a legitimate need to do so. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Information Services responsibilities

IS shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Employees shall not load removable media of unknown origin.
3. Incoming media shall be scanned for viruses before they are read.
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the Director of Information Technology.

Access Codes and Passwords

The confidentiality and integrity of data stored on the College's computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

Information Services responsibilities

The IS department shall be responsible for the administration of access controls to all College computer systems. The Information Technology Director will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor. Deletions may be processed by an oral request prior to reception of the written request The Information Technology Director will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Should change passwords at least every 90 days.
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period of time.

Human Resources responsibility

The Human Resources Department will notify the Information Technology Director of employee transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

Physical Security

It is College policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

1. Removable media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Removable media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
4. Since the IS staff is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.
5. Employees shall not take shared portable equipment such as laptop computers off-campus without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
6. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

Copyrights and License Agreements

It is Rosemont College policy to comply with all laws regarding intellectual property.

Legal reference

Rosemont College and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose Rosemont College and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by Rosemont College, licensed to Rosemont College, or developed using Rosemont College resources by employees or vendors.

IS responsibilities

The IS Staff will:

1. Maintain records of software licenses owned by Rosemont College.
2. Periodically (at least annually) scan company computers to verify that only authorized software is installed.

Employee responsibilities

Employees shall not:

1. Install software unless authorized by IS. Only software that is licensed to or owned by Rosemont College is to be installed on Rosemont College computers.
2. Copy software unless authorized by IS.
3. Download software unless authorized by IS.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

Criminal penalties

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years