Felician University
Office of Information Technology
262 South Main St
Lodi, NJ 07644-2117

Computer Use Policy

Introduction - In support of Felician University's mission of teaching and public service, the Information Technology (IT) Department provides computing, networking, and information resources to the community of students, faculty, and staff.

This policy regulates the use of all computing equipment and network interconnections owned or administered by Felician University. These include, but are not limited to, administrative computing resources, office and residence hall personal computers, devices, campus-wide computer laboratories, smart boards, network servers, thin-client terminals, laptops, iPads, and associated peripherals such as printers, scanners, copiers and fax machines.

Rights and Responsibilities - Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly and adhere to institutional policy. Users must respect the rights of other users, respect the integrity of computer and related physical resources, and observe all relevant laws, regulations, contractual obligations.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged. Institutional computers and access to institutional systems and software are for business purposes and the property of the University.

Existing Legal Context - All existing laws (federal and state) University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but those that may apply generally to personal conduct.

Misuse of computing, networking, or information resources may result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University policies or procedures. Complaints alleging misuse of computing resources will be directed to those responsible for taking appropriate disciplinary action. Unauthorized uses of any computers, networking or informational resources are prohibited.

Other organizations operating computing and networking facilities that are reachable via the Felician University network may have their own policies governing the use of those resources. When accessing remote resources from Felician University facilities, users are responsible for abiding by both the policies set forth in this document and the policies of the other organizations and networks.

Illegal reproduction of software protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fine and imprisonment.

Examples of Misuse - Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use.
- Obtaining a password for a computer account without the consent of the account owner.

Felician University
Office of Information Technology
262 South Main St
Lodi, NJ 07644-2117

- Allowing someone else to use your account. The owner of the account is responsible for the use (and misuse) of the account. The owner must take all responsible precautions, including password maintenance, to prevent use of the account by unauthorized persons. Faculty and staff with access to the University's databases must properly log in and out and when in the database - insure that only those with authorized access to the University's databases view their screen. When finished with the database, users must log out to both "free up" computer resources and guard against unauthorized access or viewing.
- Using the campus network to gain unauthorized access to any computer system
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as, computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws. This includes the broadcast distribution of copyrighted material from electronic sources.
- Deliberately or negligently wasting computer resources. This includes, but is not limited to, printing multiple copies of a document on a University-owned printer, propagating chain e-mail letters, broadcasting an e-mail message to all system users without authorization, storing large files on host computers, running programs on host computers that use a disproportionate share of system resources, and failing to sign off from a mailing list you have no interest in following.
- Using electronic mail to harass others.
- Masking the identity of an account or machine. This includes, but is not limited to, sending anonymous e-mail.
- Using University owned computing resources for any activity that is commercial in nature.
- Posting on electronic bulletin boards or Internet services materials that violate existing laws or the University's code of conduct. This includes, but is not limited to, posting obscene or sexually explicit pictures or text to a public on-line conference, or posting of materials that are slanderous or defamatory in nature.
- Attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; reading another person’s e-mail.

Felician University
Office of Information Technology
262 South Main St
Lodi, NJ 07644-2117

All faculty developing courses for on-line or distance learning must read and follow the guidelines established by the University's Distance Learning Coordinator. Presentations designed on (or run through) the University's network or non-network equipment must adhere to the guidelines established in this use policy.

Activities will not be considered misuse when authorized by appropriate University officials for security or performance testing.

Treatment of Confidential Information
Confidential information generally consists of non-public information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or damage the person or entity's financial standing, employability, privacy or reputation. The University is bound by law or contract to protect some types of confidential information, and in other instances the University requires protection of confidential information beyond legal or contractual requirements as an additional safeguard. Confidential information includes but is not limited to:

- payroll records, salary and non-public benefits information
- Social Security numbers, driver's license numbers, state identification card numbers, passport numbers
- credit and debit card information, and financial account information
- personnel records, including but not limited to information regarding an employee's work history, credentials, salary and salary grade, benefits, length of service, performance, and discipline
- individual criminal background check information
- individual conflict of interest information
- individually identifiable biometric information
- computer system passwords and security codes
- unpublished grant proposals and unpublished research data
- unpublished manuscripts and correspondence
- budgetary, departmental, or University planning information
- non-public financial, procurement, health/safety, audit, insurance and claims information
- internal investigation information, pre-litigation, and non-public litigation and administrative agency charge, audit and inquiry information
- student records, including but not limited to student education records within the meaning of the Family Educational Rights and Privacy Act
- proprietary or intellectual property in which the University asserts ownership that is created by University employees in connection with their work
- non-public law enforcement records generated or maintained by the University security offices

Felician University
Office of Information Technology
262 South Main St
Lodi, NJ 07644-2117

- all University client communications
- non-public donor and alumni information
- patient care records including patient benefit plan enrollment, claims, billing matters, and data concerning human research subjects
- medical records, personally identifiable medical information, and all information designated as "Protected Health Information" under the Health Insurance Portability and Accountability Act (HIPAA), or otherwise protected by law
- all information, materials, data and records designated confidential by a University unit, by law or by contract, including information obtained by the University from third parties under non-disclosure agreements or any other contract that designates third party information as confidential

Guidelines:

1. All employees with job duties that require them to handle confidential information are required to safeguard such information and only use it or disclose it as expressly authorized or specifically required in the course of performing their specific job duties.
2. Misuse of confidential information can be intentional (acts and/or omissions), or a product of negligence or inadvertence. Misuse includes but is not limited to:
    - Accessing information not directly germane or relevant to the employee's specifically assigned tasks
    - Disclosing, discussing and/or providing confidential information to any individual not authorized to view or access that data, including but not limited to third parties, volunteers, vendors and other University employees
    - Reckless, careless, negligent, or improper handling, storage or disposal of confidential data, including electronically stored and/or transmitted data, printed documents and reports containing confidential information
    - Deleting or altering information without authorization
    - Generating and/or disseminating false or misleading information, and
    - Using information viewed or retrieved from the systems for personal or any other unauthorized or unlawful use.
3. Employees who have been assigned personal access codes to work with systems that generate, store or manage confidential information bear the responsibility for preserving the complete confidentiality of such codes to ensure against unauthorized use by any other person. Employees who negligently or intentionally share their system passwords or accounts with anyone else for any reason will be held responsible for any resulting misuse of the system by others.

4. Employees who have any reason to believe or suspect that someone else is using their personal access codes must immediately notify their supervisor.

5. Employees are prohibited from logging onto University databases and administrative systems with their personal access codes and then permitting another person to access information in those data bases and/or systems.

6. Student education records are governed by the Family Educational Rights and Privacy Act (FERPA) and applicable University policy (see the Student Handbook) http://www.felician.edu/sites/default/files/student-handbook.pdf . FERPA-protected student education records must not be disclosed under any circumstances absent the express consent of the University student (or former student) or as authorized by the University's Legal Counsel or the University's Registrar. Although FERPA also permits the University to disclose student directory information (as defined by FERPA), no such information may be disclosed until the Office of the Registrar has confirmed that the student has not elected to block his or her directory information, as permitted by FERPA.

7. Employees are expected to:

    - Identify confidential information and materials
    - Proactively seek information regarding and comply with any restrictions on the use, administration, processing, storage or transfer of the confidential information in any form, physical or electronic
    - Learn about and comply with any procedures regarding the appropriate handling of such information and materials
    - Understand their responsibilities related to information security

8. Employees who have access to confidential information are expected to know and understand associated security requirements, and to take measures to protect the information, regardless of the data storage medium being used, e.g., printed media (forms, work papers, reports, microfilm, microfiche, books), computers, data/voice networks, physical storage environments (offices, filing cabinets, drawers), and magnetic and optical storage media (hard drives, diskettes, tapes, CDs, flash drives). Computer display screens should be positioned so that only authorized users can view confidential information, and confidential information should be discarded in a way that will preserve confidentiality (e.g., in a shred box, not in a trash can or recycling bin).

9. In many instances, employees will be required or expected to attend training relevant to the information/materials being handled. Employees who are hired into positions that require adherence to government-mandated compliance (e.g., HIPAA, Medical Compliance, grant and contract administration, pathogens or select agents) will be subject to strict procedures for handling such materials, must attend all mandated training sessions, and comply with compliance-specific policies and applicable law.

Felician University
Office of Information Technology
262 South Main St
Lodi, NJ 07644-2117

10. Employees must notify the University of any violation of these guidelines. Employees may report their concerns immediately to their supervisor, department head, or central University administration

Enforcement - Employee misuse of confidential information and/or the systems in which the information is stored is a serious breach of job responsibilities Penalties for violation of this policy may be imposed under one or more of the following; Felician University policies and regulations, the-laws of the state of New Jersey; and the laws of the United States. Penalties may include loss of access to University computing resources, either temporarily or permanently, suspension or termination.

Minor infractions of this policy will be handled by personnel from the IT Department in an informal manner. Serious violations will be referred to the appropriate University authorities for formal investigation and action according to established procedures.

☐ I HAVE READ AND AGREE TO THE FOLLOWING TERMS AND CONDITIONS

Employee Signature _____