FRANCISCAN UNIVERSITY OF STEUBENVILLE

Appropriate Use Policy

January 2025

Purpose

Franciscan University of Steubenville ("FUS" or the "University") provides access to computer systems and networks it owns or operates to FUS students, faculty, staff, alumni, and approved guests in order to promote legitimate educational, research, and administrative efforts in keeping with the University's role as an educational institution. Such access has a broad impact and imposes certain responsibilities and obligations. Users have the responsibility to use these resources in an efficient, ethical, and responsible manner, consistent with the law and the mission of the University. The purpose of this policy is to ensure the appropriate use of FUS owned or controlled computer systems, networks, communication systems, and information technology (IT) systems ("University IT Resources").

Scope

This is a University-wide policy and applies to all faculty, employees, students, guests, and all other authorized individuals ("Authorized Individuals").

Policy

General Principles

Appropriate use is always ethical, reflects academic honesty and is exercised fairly with respect to the consumption of shared resources. Authorized Individuals are expected to demonstrate respect for intellectual property, copyright and data ownership, system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and annoyance. This policy governs appropriate use of University IT Resources and is based on the following:

1. Franciscan University of Steubenville, as owner or operator of the University IT Resources, has specific proprietary rights of access, regulation of use, resource allocation, and management.

2. Authorized Individuals have reasonable expectations of access for legitimate purposes, ownership of certain intellectual property, including data and ideas, privacy from unauthorized monitoring of electronic files and intrusion, and freedom from intimidation, harassment, and annoyance.

3. Authorized Individuals have the responsibility to utilize Franciscan University of Steubenville computer facilities and University IT Resources for legitimate University purposes related to their purpose and role within the University. They must respect the rights of others to privacy and protection of their intellectual property rights, including rights in data, ideas, and copyrighted material, and freedom from intimidation, harassment, and annoyance. As an institution of higher education, Franciscan University of Steubenville is committed to providing students, staff, and faculty with the opportunity to explore the full potential of electronic communication and data-gathering to the extent that this use is ethical, consistent with the mission of the University, and does not infringe on others' rights of privacy and access to limited resources. Appropriate use of computer facilities for an educational institution extends beyond specific University-related business but can be restricted by the University to protect its mission and the rights of other Authorized Individuals.

4. The University will make reasonable efforts to ensure that the privacy and security of Authorized Individuals is protected. However, no Authorized Individual should expect that his/her University electronic mail or personal electronic mail, if accessed using University equipment, is private. Furthermore, the University cannot guarantee that the University IT Resources are completely secure or invulnerable to attack. By using the University IT Resources, each Authorized Individual assumes the risks of invasion of privacy and misappropriation of confidential information or material that may be protected by copyright and other intellectual property rights.

University Rights of Access

As owner or operator of the University IT Resources, Franciscan University of Steubenville has proprietary rights of access, regulation of use and resource allocation and management. The University may exercise these rights when it deems it appropriate and in the best interests of the University. These rights include, but are not limited to, the following authority:

1. To make and retain copies of University-owned or controlled data, including e-mail and any other files deemed appropriate, for a time period determined by the University;

2. To access all files maintained on University equipment, including e-mail, for specific authorized purposes, including, but not limited to:
   a. To review files for resource management. This may include analysis of corrupt files, potential threats such as viruses or other malware, or files that consume an inordinate amount of resources. This review shall be by file characteristics only, such as origination date, frequency of use, or some other resource management criterion, rather than the file subject matter. In such a case, University Information Technology Services will make a reasonable effort to contact the user before any action is taken.
   b. To investigate an allegation of violation of law or University policy or in response to a subpoena. In the case of a subpoena or an allegation of violation of law, authorization for such access must be provided by the Office of Legal Affairs. In the case of an allegation of violation of University policy, authorization for such access must be provided by the Office of Legal Affairs in consultation with: (1) Human Resources, if the allegations involve an employee, (2) Academic Affairs, if the allegations involve a faculty member, or (3) Student Life, if the allegations involve a student. Allegations regarding guests or other Authorized Individuals shall be referred directly to the Office of Legal Affairs.
   c. To protect legitimate business needs, such as when an employee is unexpectedly absent for an extended time and another employee must assume the absent employee's projects or operational responsibilities. Authorization for such access must be provided by the Office of Legal Affairs in consultation with Human Resources or Academic Affairs, as applicable.

3. To remove files from University systems, including but not limited to the following reason:
    a. To conserve limited resources in accordance with established procedures. These procedures may be based on origination date, frequency of use, file size, or other resource management criteria, including the nature of file content. Authorized resource managers will make their best effort to notify file holders of these procedures before removing such files.
    b. To purge from University systems illegal files or files that infringe or may infringe on the rights of other users or third parties by inequitably consuming limited resources, abrogating creative property rights, or invading privacy (including harassment, intimidation, or annoyance).
    c. To perform other necessary resource management, after making best effort to notify the file holder.
    d. To limit or otherwise restrict creation or file size of email, Web pages, network storage, or other resource allocation to Franciscan University of Steubenville faculty, students, staff, and alumni or other specifically authorized users of University facilities, as system capacity permits. In doing so, the University seeks not to restrict expression of diverse opinions or viewpoints, but to ensure the efficient management of the University IT Resources.

4. To manage the University's voice, data, and video bandwidth to maintain the integrity and robustness of University-owned communications equipment, data, and services as well as the appropriateness of bandwidth use.

These proprietary rights of the University, as applicable, will extend to electronic messages, data or files that are sent or received on a personal, password-protected account on a web-based communication system (such as e-mail, text messaging, and file sharing services) if University-owned equipment is used to access such a personal account, to the extent permitted by law.

The University is not liable for loss of data because of systems failures, emergencies, or the unauthorized access, use, or corruption of data by any individuals, including University employees.

Denial of access privileges to University computer files and facilities shall be made only in accordance with this and other University policies and procedures applicable to the Authorized Individual. Access privileges, however, are subject to the availability of such files and the University does not warrant, guarantee, or ensure that files will be preserved or free from corruption due to human error, equipment failure or the need to purge files for resource allocation purposes.

User Responsibilities

Authorized Individuals have the responsibility to utilize Franciscan University of Steubenville computer facilities and University IT Resources ethically, with respect for other Authorized Individuals and the limited resources made available to them by the University.

This includes:

1. Being responsible for all activities performed under their user ID and for all use of resources assigned to them. The sharing of user IDs and passwords is strictly prohibited. Using the user ID of another Authorized Individual is strictly prohibited. Authorized Individuals are responsible for securing their user IDs and passwords to prevent unauthorized access.

2. Being courteous and considerate in using all University IT Resources. Authorized Individuals should be sensitive to the needs of others and use only what a reasonable person would consider a fair share of computing, network, and telephone resources, as determined at the sole discretion of the University.

3. Respecting the rights of others to privacy, including freedom from intimidation, harassment, and annoyance. Authorized Individuals must abide by University guidelines for the distribution of e-mail and may not persist in corresponding with others if they have been notified to cease.

4. Respecting the intellectual and creative property of others, including data, ideas, and copyrighted material. Use of another person's creative property without proper attribution, consent, or permission may be considered plagiarism under University policy and may constitute a violation of copyright or other laws.

5. Following best practices in the transmission and storage of University confidential information. Users must appropriately protect any confidential University information they have on their computers. Users should take particular care to protect sensitive and protected data when using public computers, laptop computers, external storage devices (such as external hard drives or flash drives), and home computers, and when emailing or posting such data to third party file sharing services.
6. Never representing that their personal comments reflect those of the University without the University’s express written consent and approval.
7. Never using University-owned trademarks unless expressly authorized by the University and only in a manner consistent with the University’s guidelines for proper trademark usage.

User Expectations

Authorized Individuals of Franciscan University of Steubenville computer and network facilities and University IT Resources for legitimate purposes have reasonable expectations of:

1. Access to properly stored files under their access privileges and access to all FUS computer files and facilities that are relevant to the legitimate and appropriate use of such University facilities. All Authorized Individuals are responsible for frequently and appropriately backing up all data to guard against such possibilities.

2. Respect for the ownership of intellectual and creative property, including data and ideas, in accordance with the United States Copyright Act and all relevant state and federal laws regarding intellectual property and data ownership.

3. Limits on the receipt of certain kinds of communications. The University will attempt to strike a balance between the Authorized Individual's interest in limiting receipt of certain kinds of communications and the interests of other Authorized Individuals in reaching an appropriate audience. To this end, the University will encourage the use of managed organizations (such as those available in the campus portal or the campus learning management systems) for general-purpose communications and the use of approved broadcast facilities when they are of potential interest to large numbers of community members. Authorized Individuals are expected not to send information except to recipients they reasonably expect to welcome such communications and are expected to honor requests from recipients not to receive further communications.

Authorized Individuals should not expect the privacy of personal electronic mail or other Web based communications, or of content residing on or transmitted through University equipment and University IT Resources. The content of electronic messages and files sent or received through personal accounts on Web-based services such as email, text messaging services, file sharing services, or social media sites often leave copies on the equipment used; if University equipment and University IT Resources is used to access such private accounts, the University to the extent provided by law reserves the right to access and disclose such content without the consent of the Authorized Individual.

Inappropriate Uses

Examples of inappropriate uses of Franciscan University of Steubenville computer facilities and University IT Resources include, but are not limited to:

1. Commercial uses not specifically authorized by the University.

2. Copying any University-owned software for any purposes, unless specifically authorized by the copyright and licensing provisions of the software and approved by the University.

3. Any circumvention of Franciscan University of Steubenville computer security, including using another Authorized Individual's password, decoding passwords, misrepresentation in order to obtain access to data or computer systems, or otherwise devising unauthorized access.

4. Activities that damage or disrupt hardware or communications, such as irresponsible or destructive use of equipment, the use of unauthorized network equipment, including the use of unauthorized wireless equipment, virus creation and propagation, wasting system resources, and overloading networks with excessive data.

5. Intentional damage to or altering of systems, software, or information owned by others, including individual and University files, except as specifically allowed by the file holder.

6. Using University IT Resources to access any other computer system (on- or off-campus) without authorization.

7. Sending offensive, harassing, or threatening messages or repeated sending of unsolicited e-mail after being asked to stop.

8. Illegal use of downloaded copyrighted materials including text, audio, and video. It is illegal to download or share copyrighted material that has not been approved for such distribution and such downloading of copyrighted material is a violation of this and other University policies and will lead to corrective action at the discretion of the University.

9. Disseminating any confidential information unless such dissemination is required by the Authorized Individual's job at the University and is done securely, as determined by the University IT Department and Office of Legal Affairs.

Non-Compliance

Any violation of this policy may be referred to the respective University Vice President or Executive Director (for Student Life, Human Resources, and/or Academic Affairs) to address the allegation in accordance with the applicable student, employee, and/or faculty handbooks. Such violations will be subject to appropriate corrective actions including, but not limited to, termination of the Authorized Individual’s relationship with the University.

Periodic Review and Future Revisions

This policy will be periodically reviewed and revised at any time as needed. FUS may apply policy revisions to an active case provided that doing so is not clearly unreasonable.