Information Technology Policies and Procedures - Students

Purpose

This policy outlines the principles and guidelines that govern the use of Franciscan University of Steubenville's (the University) Information Technology resources and services. There are two primary purposes for the policies contained herein:

To protect the University network, private information of the University, and all personal information that has been entrusted to the University.

To ensure that the University network, and associated resources, are available for the employment and academic needs of all members in the University Community.

IT Resources are provided by the University for the advancement of the University's mission in its operational, outreach and academic objectives. Any access or use of IT Resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of these policies.

Scope

This policy and all policies referenced herein, shall apply to all students who use, access, or otherwise employ locally or remotely, the University's IT Resources, whether individual controlled, shared, stand-alone, or networked.

Franciscan University of Steubenville advises everyone with authorized access to follow these policies and to conduct themselves within the framework of the University's Mission Statement.

Enforcement

Anyone found to be negatively affecting the operation of the University network, the security of the University network, private information of the University, or personal information of its constituents will be contacted by Information Technology Services (ITS) with notification of the problem and a request to address the specific issue. In some instances, problems may arise that a student is completely unaware of. The student is still responsible for addressing the problem with the assistance of ITS. If the problem persists, it will then be handled in accordance with policies outlined in the student handbook.

Revisions

The policies within this document will be updated on an ongoing basis as student and institutional needs change and in keeping with Information Technology best practices.

FRANCISCAN UNIVERSITY OF STEUBENVILLE

TABLE OF CONTENTS

DEFINITIONS

AUTHENTICATION: The process or action of verifying the identity of a user.

AUTHORIZATION: A security mechanism used to determine user privileges or access levels related to system resources including computer programs, files, services, data and application features.

IT RESOURCES: Computing, networking, communications, application, and telecommunications systems, printing, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

MALWARE: Short for "Malicious software", malware refers to software programs designed to damage or do other unwanted actions on a computer system. Ex: viruses, ransomware, worms, Trojan horses and spyware.

NETWORK: A group of two or more devices that can communicate. A network is comprised of computer systems and devices that are connected by physical and/or wireless connections and allow computers and/or individuals to share information and resources.

TWO-FACTOR AUTHENTICATION: A security mechanism in which individuals are authenticated through more than one required security and validation procedure. For example, when logging into Office 365, username and password must be entered as well as a code that the user receives via an authenticator app, text message or phone call.

USERS: All students who use, access, or otherwise employ locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

POLICY

Section 1: Authorization

Access and use of Franciscan University IT Resources are limited to authorized Users for the purposes that are consistent with the operational, outreach and academic goals of Franciscan University within the framework of the University's mission. All authorized Users will act in good faith to protect the security and integrity of the information and systems for which they are entrusted.

Authorized student users will be provided with login credentials for the Franciscan University IT Resources by Information Technology Services. Access is granted to students that are deemed to be active in accordance with the Account Provisioning Policy (see section 4).

Every authorized User shall have a unique username and password to access all University IT Resources. These credentials should not be shared with any other person for any reason whatsoever.

Section 2: Account Security

Your password provides the key to open your account, various software applications and the Franciscan University wireless network. The importance of safeguarding your password cannot be stressed enough. Your password should be kept private and should be stored in a secure location. Passwords must not be prominently displayed or taped to any computer or device.

Passwords should be unique for every software application that you log in to. The one exception is AccessFUS, which is specifically designed to allow a single username and password to log in to multiple systems; this password should be unique from all other passwords. If your username and password are breached, a unique password will ensure that the malicious party cannot use your credentials to log in elsewhere.

Your Franciscan University account password should conform to the following password standards.

- May not contain the User's account name, first or last name
- May not contain the word *password*
- Must contain at least twelve characters from three of the following categories:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Must be changed every 90 days
- Must be used for at least 2 days

Two-factor authentication will be enabled for all software applications that provide this functionality. By default, two-factor authentication is enabled for all Office 365 accounts.

Section 3: Student Responsibilities

Students are prohibited from using any portion of the IT Resources to access, print, post or distribute any information that violates the University's mission. IT Resources may not be used for political campaigns, fundraising, commercial enterprises, mass mailings, or other outside activities that have not been specifically granted the use of the University's IT Resources.

Students shall not use file sharing or peer to peer programs, including, but not limited to Usenet, Kazaa, Morpheus, Gnutella, BitTorrent, eMule, etc. to illegally download, retrieve or share files. For further information on copyright infringement and file sharing, please review **Appendix A: Addendum to the Higher Education Opportunity Act of 2008**.

Students shall never use the University's IT Resources to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer, server or network facility anywhere. Users shall never knowingly endanger, or attempt to endanger, the security of any University computer, server or network facility.

Students shall never attempt to modify or disrupt the configuration or operation of University software. This includes automatic system updates, anti-virus scans, personal firewall settings, or any other process initiated by ITS. Authorization from ITS is required to install any software on University owned computers.

Students may not modify or tamper with any University owned hardware including any device, network wiring, wall faceplates, or network devices. Setting up networks by attaching a wireless access point, hub, router or switch to the network is not permitted. Users are prohibited from setting up their computers to be used as DHCP, DNS, File Sharing, web or FTP server. Computers cannot be set up to act as a bridge, router, or gateway.

Section 4: Account Provisioning and De-provisioning Policy

Student access to the University network and systems is enabled by ITS once a student has been admitted to the University and will remain active until 30 days after graduation. For students that withdraw or do not return for subsequent semesters, their account is disabled. Further details are listed below.

Students

Activation: Upon being admitted to the University.
De-activation:

- Graduating students:
  - 30 days post-graduation, a student's account will be de-activated. Prior to their account being de-activated, it is the student's responsibility to download any files or emails from their Office 365 account that they would like to retain.
- Non-returning students:
  - At the beginning of each semester, all students that are not enrolled and registered for classes will be deemed inactive and their accounts will be de-activated.
  - The student email account will no longer receive email once the account has been de-activated.
  - It is the student's responsibility to download any files or emails that they would like to retain.

Student Workers
Activation: Upon being hired and with presentation to ITS of an approved work agreement.
De-activation: All student employee accounts are de-activated at the end of each term. If a student continues their employment in subsequent semesters, their account will be re-activated upon presentation of an updated and approved work agreement.

Employees that are also Students
Employees that are also students will be provided with separate student and staff accounts.

- For as long as the employee remains a student, their primary email account will be their employee account and used for all communications within the University.
- If they are no longer employed by the University, the staff account will be de-activated according to the policies pertaining to employees. If the former employee remains a student of Franciscan University, all email communication will be sent through their student email account.

Section 5: Internet Access

Franciscan University provides Internet access for all authorized students through the Residential Network (Resnet), administered through Information Technology Services. When connecting to this network through a personal device or through a computer in one of the University labs, students must adhere to all relevant policies contain within this document.

The University reserves the right to remove Resnet Users from the network without cause or notification. This removal may be permanent if the User is in violation of any of the policies or procedures stated within this policy document, the student handbook or other relevant University policies and procedures. Violations of these policies incur the same type of disciplinary measures as violations of other University policies, or state/federal laws, including criminal prosecution in serious cases. Violations constitute misuse of University property.

Section 6: Content Filtering

In accordance with Franciscan University's mission, Information Technology Services enforces restrictions that filter out certain internet content that is inappropriate or unacceptable. By restricting access to various sites, the University safeguards against material that can prove to be malicious, harmful and/or immoral and does not enhance the dignity of the human person. Specific sites pertaining to violence, pornography, cults, drugs, gambling, militant, and extremist hate groups, and other inappropriate sites are not accessible to students through Resnet.

We urge the students to refrain from accessing inappropriate sites and encourage them to use the Internet as a resource for academic growth and to govern themselves within the framework of the University's mission.

Section 7: Electronic Transmission of Data

Users are responsible for every message they transmit through their University account and are prohibited from using the University's network, software applications and/or email account to transmit any communication prohibited by law or that violates University practice, policy or the spirit of its mission.

Your Franciscan University student email address will be used by faculty and staff for all official email communication related to your coursework, administrative matters and University announcements. This email address should also be the primary email account to communicate with your instructors as well as the various departments and staff members of the University.

University email cannot be automatically forwarded to external addresses as this circumvents the ability to enforce proper security policies on these messages and prevents ITS form providing a guarantee that messages have been received in the intended mailbox.

Section 8: Computer Lab Use

Computer labs are available in Cosmas & Damian Hall, Egan Hall and the St. John Paul II Library. All students must adhere to the University Acceptable Use Policies while using the IT Resources available in these spaces.

Students are not permitted to load any software or games on any computer in the computer labs. All software must be approved and installed by a representative from Information Technology Services. If software is found to be installed on a lab computer that was not authorized by a representative from ITS, ITS has the right to remove that software at its discretion.

The lab computers are reset on a regular basis such that any documents that have been saved to the computer are deleted. As such any personal documents should be saved to OneDrive or a flash drive (thumb drive).

Game playing, other than those assigned specifically for course work, is not allowed in the labs at any time.

No materials or equipment may leave the computer labs, under any circumstances, without the written permission of an ITS staff member.

It is the User's responsibility to log off the lab computer when they are finished working. Failing to log off may result in the User's information being compromised.

Appendix A: Addendum to the Higher Education Opportunity Act Regarding Copyright Infringement and File Sharing

The Higher Education Opportunity Act of 2008 (HEOA) added provisions to the Higher Education Act of 1965, as amended, (HEA) requiring institutions to take steps to combat the unauthorized distribution of copyrighted materials through illegal downloading or peer-to-peer distribution of intellectual property. These requirements were effective upon enactment of the HEOA, August 14, 2008. On October 29, 2009, the Department published final regulations implementing the statutory requirements (74 FR 55902). These regulations are effective July 1, 2010.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

All damages and penalties will be taken against those individuals who engage in illegal downloading or unauthorized distribution of copyrighted materials using the University's network. Franciscan University of Steubenville will not assume any responsibility regarding damage and penalties for individuals who engage in illegal downloading or unauthorized distribution of copyrighted materials using the University's network.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.