FRANCISCAN UNIVERSITY OF STEUBENVILLE

INFORMATION TECHNOLOGY POLICIES AND PROCEDURES – EMPLOYEES

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 faculty, staff, student workers, vendors, guests and independent contractors (the Users) who use, access, or otherwise employ locally or remotely, the University's IT Resources, whether individually 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.

Any software or IT Resource need for a specific operational, outreach and academic purpose that conflicts with this policy should be discussed with the Director of Information Technology Services to determine how to best accommodate the need.

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 the Director of ITS with notification of the problem and a request to address the specific issue. In some instances, problems may arise that an employee is completely unaware of. The employee 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 appropriate faculty or staff handbook. Issues involving non-employee Users will be addressed directly by the Director of ITS or in collaboration with other division or departmental leaders as deemed necessary based on the severity of the incident.

REVISIONS

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

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.

Personal Use: In the context of this policy document, personal use of IT Resources encompasses any activity unrelated to the operations, outreach or academic endeavors of the University. The use of IT Resources for conducting research, storing intellectual property, creating class content or other activities related to academic endeavors of a faculty member for the University are not considered personal use.

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 faculty, staff, student workers, vendors, guests and independent contractors who use, access, or otherwise employ locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Virus: A malicious computer program that can copy itself and infect a computer. A virus can spread from one computer to another when transferred to the target computer through an email attachment, file transfer over a network or the internet, or with a portable storage medium such as a USB drive or external hard drive.

Guidelines

Section 1: Guidelines for Personal Use

Except for explicitly stated personal use policies, employees are responsible for exercising good judgment regarding the reasonableness of personal use of Franciscan University IT Resources. University owned computers and devices are intended to be used for matters related to the operations, outreach or academic endeavors of the University.

Any material that is personal in nature and unrelated to the operations, outreach or academic endeavors of the University should not be stored on a Franciscan University network drive or shared storage medium and will be subject to removal at the discretion of Information Technology Services.

Franciscan University is not responsible for the backup, security or integrity of any personal information nor for any personal applications that are installed on University owned devices.

If personal use is deemed to be excessive, as defined by your direct supervisor, and/or if your personal use interferes with normal operation of the University network, systems or applications; or poses a significant security concern, the issue will be brought to your attention through your direct supervisor or the Director of Information Technology Services. The issue will be handled in accordance with policies outlined in the faculty or staff handbooks.

Policy

Section 2: 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.

Once approved through the appropriate process, authorized Users are provided with login credentials for IT Resources by Information Technology Services. Access is granted to Users that are deemed to be active in accordance with the Account Provisioning Policy (see section 6) and will be provided based on the demonstrated need to access information or perform a specific function.

Every authorized User shall have a unique username and password to access all University IT Resources. It is against University policy and our software licensing agreements to create a general account intended to be used by multiple Users through sharing of the username and password.

With approval from ITS, vendors may be granted limited access to Franciscan University IT Resources. Vendor accounts must also be unique for every individual; generic/group accounts will not be created. All vendor account holders are subject to all policies contained within this document. Vendor accounts may only remain active while access is required and must be de-activated at the conclusion of the project, partnership or when access to the system/data is no longer required. It is the responsibility of the department/division leader to ensure that vendor access is maintained in accordance with this policy.

Section 3: Account Security

Your password provides the key to open your account as well as access to all systems and information that you have been entrusted with. 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.

All passwords used to access software applications owned by Franciscan University should conform to the following password standards.

- May not contain the User’s account name or their full name.
- 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.
- The last 24 passwords cannot be repeated.

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.

To protect against unauthorized access, user accounts are automatically locked for 30 minutes after 10 invalid login attempts. Contact ITS for assistance and to report any unusual activity on your computer.

Section 4: User Responsibilities

Users 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.

Users shall not use shared University computers for unauthorized games, chat rooms, or other multi-user recreational sites for personal interest, as these may unintentionally invite a malicious party into our network. Faculty assigned games and chat rooms to teach particular concepts can be used with prior coordinated authorization from the Manager of User Support Services. Questions regarding the use and installation of particular software programs should be directed to the Director of Information Technology Services.

Users 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**.

Users 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.

Users 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.

Users 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 5: Account Provisioning and De-provisioning Policy

Employee access to the University network and systems is created by ITS at the request of the Human Resources department and coincides with the employee's first day of employment. When an employee leaves the University, their account is de-activated at the close of business on their last day of employment. Access to the Franciscan University network, Office 365 (including email), and credentials to log in to any University system or application is de-activated at that time. Further details are listed below.

Full-time Faculty
Activation: Hire date
De-activation: Close of business on the last day of employment, unless otherwise directed by HR.

Adjunct Faculty
Activation: Hire date
De-activation: Close of business on the last day of employment, unless otherwise directed by HR. The list of active adjunct faculty will be reviewed at the beginning of each semester to determine active status. ITS will work with Academic Affairs and Human Resources to determine which accounts should remain active on a semester-by-semester basis.

Staff
Activation: Hire date
De-activation: Close of business on the last day of employment, unless otherwise directed by Human Resources.

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. Accounts are activated each semester upon presentation of an approved work agreement.

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

- 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 account.

Vendors/Independent Contractors
Activation: Upon completion and approval of the Vendor Access to IT Resources form.
De-activation: Upon completion of the vendor contract/project or termination of the user's employment.

Section 6: Data Classification

Franciscan University's Data Classification Policy applies to all data produced, collected, stored or used by the University, its Users during their relationship with the University. All data covered by the scope of this policy will be classified as protected, sensitive or public data.

Users are responsible for adhering to all applicable laws that govern the use and protection of data. These laws include, but are not limited to: FERPA, GLBA, HIPAA, GDPR and PCI standards. See **Appendix B** for more information on these data privacy laws and regulations.

Access to data is assigned on a least privilege basis, meaning that minimum permissions to information are assigned based on the job responsibilities of the User. Data access can be requested using the "Data Access Request Form" on MyFranciscan under the ITS Help tab.

6.1 Data Classification Types:

Protected Data

Protected data is any information that relates to a person and that could be used, either directly or indirectly, to identify or contact such person, whether a natural person or a legal entity, including, without limitation, (a) an individual's Social Security number; or (b) any combination of any individual's name (including first or middle initial and last name) and any one or more of the following data relating to such individual: (i) individual taxpayer identification number, driver's license number, passport number or any other government-issued identification number; (ii) account number (including any credit card number, debit card number, or other financial account number, as well as any other Franciscan University account number); (iii) medical or health information or records; (iv) an individual's user name or email address in combination with a password or security question and answer that would permit access to an online account; (v) data obtained from a consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (vi) data elements revealing race, ethnicity, national origin, religion, trade union membership, sex life or sexual orientation, and criminal records or allegations of crimes, and (vii) any Personally Identifiable Information (PII) as defined under COPPA (15 U.S.C. Ch. 91; §6501 et seq.) and FERPA (20 U.S.C. §1232(g) et seq. and 34 C.F.R. Part 99.3).

These regulations may include, but are not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)
- General Data Protection Regulation (GDPR)
- Children's Online Privacy Protection Act (COPPA)

Additional information on the above privacy laws is available in **Appendix B: Data Laws and Regulations**.

Sensitive data

Data that is not classified as protected data, but that is classified by the department originating or maintaining custody of the data as being proprietary information. Custodians or owners of data classified as sensitive data identify this information as sensitive based on their internal standard operating procedures. Examples of the type of data included are budgets, salary and raise information as well as possible investments that Franciscan University may be interested in pursuing.

Public data

Data that Franciscan University intends to make available to the general public. Examples of these types of data include, but are not limited to, department faculty lists, department addresses, press releases and the Franciscan University website. Data that does not contain PII concerning any individual and that is not protected data or sensitive data, is classified as public data.

Section 7: Data Storage and File Sharing

Any information related to the operations of the University must be stored within University owned applications, shared network drives or other shared storage as designated by Information Technology Services. For faculty, any Information that is deemed to be intellectual property, is related to faculty research, class content or other activities related to academic endeavors may be stored in alternate locations at their own risk. Information Technology Services does not have the ability to back up this information and will not be responsible for the recovery of information stored outside of University shared network drives or Microsoft One Drive.

Authorized Users may use the University shared network drives or Office 365 OneDrive for Business to store information related to the operations of the University. OneDrive for Business is the only document sharing platform that is authorized for sharing documents within and outside of the University. No other file sharing services (Box, Dropbox, Google Drive, Apple iCloud etc.) should be used. Your University email may continue to be used to distribute and share documents, as appropriate, with others.

Any protected or sensitive data, as defined above in section 6 is prohibited from being stored directly on any mobile device (mobile phone, laptop, tablet, iPad, flash drive, external hard drive, CD, DVD etc.) Any protected or sensitive data that is stored in OneDrive should not be synchronized to any other device.

Any protected or sensitive data is prohibited from being shared with any User that has not been granted explicit permission to see or use that information.

Any protected or sensitive data is prohibited from being shared with any party outside of the University through email or file sharing services such as OneDrive. Contact ITS for alternate methods of sharing this information securely when necessary.

Information Technology Services has the right to scan all documents for data protected by privacy laws and regulations that are stored within shared network drives, University file sharing services and all University owned devices. This type of scanning provides Information Technology Services staff with a report of users and document names that may contain protected or sensitive information. This information will be communicated to the user to ensure that all protected or sensitive information has been shared or distributed in accordance with University policies.

Users are prohibited from storing their Franciscan University credit card information on their personal or University owned computer or mobile device (laptops, smart phones, tablets, iPads, etc.).

Users are responsible for all data stored locally on their laptop or desktop. Users should take care to ensure that all Franciscan University related materials are stored in Office 365 OneDrive or on the user's corresponding network drive as this drive is archived and backed up regularly. Users are responsible for backing up any data on their laptop or desktop's local drive. The University is not responsible for any data stored locally on computers.

Section 8: 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 email address must be used only for operational, outreach and academic matters related to the University. The use of any other email account is not permitted when communicating on behalf of the University.

Your Franciscan University email address may not be used for the purchase of software, subscriptions or any online account that is personal in nature or unrelated to the operations, outreach or academic endeavors of the University. When a data breach occurs for a vendor where your University email address has been used in conjunction with a password that is the same or similar to your University password, your University account can easily be compromised.

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.

Users shall not attempt to read, alter, or delete anyone's email other than their own unless given the proper permission through proxy access or authorized internal forwarding.

Any information that is protected by data privacy laws and regulations should never be sent via email, nor should it be shared externally with anyone via a file sharing service, including OneDrive. Contact ITS for alternate methods of sharing private information when necessary.

Section 9: Network and Device Security

Information Technology Services is responsible for the overall maintenance and security of the University network and software applications. Every authorized User is responsible for the security of their account including all usernames and passwords, their Franciscan University owned computer and mobile device, where applicable, as well as all electronic information and documents that they have been entrusted with.

All authorized Users are required to participate in periodic security awareness training to be completed in a specific timeframe. If the training is not completed within the timeframe specified, the Director of ITS will provide notice that your University account will be suspended until such time as the training is completed.

Effective January 2020, Franciscan University will only allow Office 365 account (email, OneDrive, Word, Excel, OneNote, etc.) access from a mobile device (iOS or Android) once Mobile Device Management is configured on that device. This includes Franciscan University-owned as well as personal devices and will require that your mobile device is protected by a password. For more information, see the "What is Mobile Device Management?" information on the ITS Q & A web page. Upon termination of employment, your Office 365 account and data stored within that account will be removed from your mobile device through the Mobile Device Management software.

Users are required to lock their computers prior to leaving their work areas. If a computer is left idle for 10 minutes, the computer will automatically lock, requiring that your password be entered to regain access to the device.

Users are responsible for taking precautions to ensure that any information or file that they access, transmit, and/or download is free from any computer code, file, or program that could negatively impact other University IT Resources. Any security risk should be immediately reported to ITS.

Section 10: Computer/Mobile Device Policy

Every employee that is provided with a University computer or mobile device is responsible for the physical security of their assigned computer/device and is expected to take due care in the handling and use of these resources.

On an annual basis, Information Technology Services selects standard PC and Mac models for employee use. All devices are purchased or leased based on the requirements of the employee's job responsibilities. Any request to purchase/lease a computer outside of the standard specifications must be accompanied by a justification from the employee and authorized by their department/division leader.

Employees that have been allocated a leased laptop must read and acknowledge the Faculty Lease Agreement. A signed copy of this agreement must be provided to ITS prior to receiving the leased laptop.

All Users must exercise due care in the handling and use of their assigned computer/device. Costs related to damage outside of regular wear and tear and not covered by the manufacturer's warranty will be the responsibility of the user. ITS should be contacted in the event that a University computer/device is damaged or not operating properly to facilitate the repair.

Users are expected to take every precaution to ensure the computer/device's security and proper use. If a computer/device is lost or stolen, ITS should be contacted immediately, as well as campus security or local law enforcement. In the event of negligence in the management of the computer/device, the University is under no obligation to provide a replacement and the User may be personally responsible for any financial obligations incurred by the University.

University computers and mobile devices are provided to employees for the purpose of fulfilling their job responsibilities and should only be used by authorized Users.

All computers/devices must be maintained in such a way that they can be connected to University networking facilities for access to the Internet, library resources, the Jenzabar One student information system as well as any other systems required to perform your job duties.

Employees should ensure that their computers are configured with the hardware and software specifications recommended by ITS, including anti-malware and anti-virus software (with regular updates applied). The anti-malware software is to be configured to fully scan the User's computer on a regular basis for known malware. Any updates and services to the resources given to User are to be applied by ITS.

Users must comply with all application and/or software license agreements acquired by the University and its authorized units.

There shall be no unauthorized hardware upgrade to the standard configured computer without the consent of Information Technology Services.

Upon termination of employment with the University, Franciscan University owned computers/devices must be returned immediately to ITS. Any employee that fails to return their computer/device will be held personally responsible for the total replacement cost of the computer/device.

Section 11: Remote Access

Franciscan University employees with a University-owned desktop, laptop, or other mobile device may request permission to connect remotely to the University's network for the purpose of conducting business related to the operations, outreach or academic endeavors of the University.

Any University employee that is granted remote access privileges to the campus network is subject to the same policies and procedures that apply to the use of the same resource while on campus and connected to the University network, as contained in this policy document.

Users requiring remote access to/from a University computer/device must review and acknowledge understanding of the University's Remote Access Policy. This access must be approved by the User's department leader/vice president and the Director of Information Technology Services.

The Remote Access policy is available on MyFranciscan under the "ITS Help" tab through the "Online Forms" link.

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 were 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.

Appendix B: Data Laws and Regulations

The **Family Educational Rights and Privacy Act** (FERPA) covers all student data. The University can disclose without consent directory information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance as long as the student's disclosure preferences are honored. If any data is present that has been flagged for nondisclosure, or if the disclosure option is not checked and enforced, the data (along with all other student data that is not considered directory information) is considered sensitive. Additional information is available at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

The **Gramm-Leach-Bliley Act** (GLBA), includes privacy provisions to protect consumer information held by financial institutions. Because of student loan activity, a university is considered a financial institution under the GLBA. FERPA compliance places the University in compliance with the Federal Trade Commission privacy rules under the GLBA. Additional information can be found at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) is a federal law establishing national standards for the privacy and security of an individual's health information. This is information created or received by a health care provider or health plan, including health information or health care payment information plus information that personally identifies the individual patient or plan member, including:

- A patient's name and e-mail, Web site and home addresses
- Identifying numbers, including Social Security numbers, medical records, insurance numbers, biomedical devices, vehicle identifiers, and license numbers
- Full facial photos and other biometric identifiers
- Dates, such as birth date, dates of admission and discharge, or date of death

Additional information can be found at http://www.hhs.gov/ocr/hipaa/

Payment Card Industry (PCI) Standard is a contractual agreement between a university and its merchant bank. The agreement covers handling of credit card numbers, magnetic stripe contents, card verification code numbers, and expiration dates. In addition to the standards outlined above for sensitive systems, PCI requires extra security and has its own set of standards. Additional information is available at https://www.pcisecuritystandards.org/tech/index.htm

The **General Data Protection Regulation** (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue-based. The General Data Protection Regulation covers all companies that deal with data of EU citizens. GDPR came into effect on May 25, 2018. Additional information is available at https://eugdpr.org/

The **Children's Online Privacy Protection Act** (COPPA) is a federal law that prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. Additional information is available at https://www.law.cornell.edu/uscode/text/15/6501