Faculty Handbook

Volume 2017 *2017-2018* Article 34

2017

3.4 Technology Use Policy

Saint Mary's College of California

3.4 TECHNOLOGY USE POLICY

Saint Mary's College of California ("Saint Mary's") is a non-profit public benefit corporation dedicated to offering a Catholic, Lasallian, Liberal Arts education. Saint Mary's has developed Information Technology (IT) resources to support this mission. This Policy governs the appropriate use of Saint Mary's IT Resources.

1. The primary purpose of Saint Mary's IT Resources is to facilitate and support the Academic Mission of the College.
2. The use of Saint Mary's IT resources for College business and operational activities such as Financial and Academic administration, student support, and facilities administration are also critical in support of the Academic Mission of the College.
3. The mission-aligned priorities noted above constitute the primary use of Saint Mary's IT Resources. All other uses are secondary, and must not interfere with primary use of Saint Mary's IT Resources
4. The use of Saint Mary's IT Resources is a privilege that is extended to all qualified members of the Saint Mary's Community, and must be consistent with the priorities listed above.
5. The use of Saint Mary's IT Resources by all Users must comply with all applicable laws and Saint Mary's Policies. Violations may result in suspension or termination of User privileges.
6. By accessing Saint Mary's IT Resources, Users implicitly agree to abide by this Policy.

This section contains several related IT Policies
Saint Mary's College of California General Policies Governing the Use of Information Technology
Saint Mary's College of California Policy Governing the Attachment and Use of Personally-owned Computing Equipment on the Saint Mary's Network
Saint Mary's College of California Policy for College-Provided Mobile Computing Equipment
Saint Mary's College of California Password Policy
Saint Mary's College of California Web and Blog Use Policy
And refers to the Saint Mary's Institutional Security Policy and to federal copyright law

3.4.1 GENERAL POLICIES GOVERNING THE USE OF INFORMATION TECHNOLOGY

3.4.1.1 IT Policy Governance

This and other IT Related Policies (listed below under "Related Policies") are subject to amendment or revision as appropriate by approval of the Technology Planning and Policy Committee (TPPC).

3.4.1.2 Scope

This and other Related IT Policies apply to all users (Users) of Saint Mary's IT resources, including faculty, staff, students, campus visitors and contractors, and apply whether the user is accessing these resources while on campus or remotely over the internet.

3.4.1.3 USING INFORMATION TECHNOLOGY RESOURCES

3.4.1.3.1 General

The use of IT resources shall be consistent with the mission of the College, College policies, and must not violate Federal, State or local laws or regulations. (Note: For questions regarding copyright and trademark issues, Fair Use, or other legal matters relating to the use of copyright-protected materials on the Saint Mary's network, please refer to the Saint Mary's Library Resources web pages. Legal questions about such issues should be directed to your Dean, area Vice President or Vice Provost, who can consult about your question with College Counsel, if necessary.)

3.4.1.3.2 Access

IT resources are available to Users on campus as well as remotely through the internet, twenty-four hours a day, and seven days per week. Technical support is limited to academic business hours, and Saint Mary's may on occasion temporarily interrupt this availability to conduct ordinary as well as extraordinary business and maintenance.

3.4.1.3.2.1 Faculty and Staff

Use of IT resources is limited to that which is necessary as part of a User's duties, responsibilities and mission-related activities. Incidental personal use during a User's working hours where such use does not interfere with a User's performance, does not violate any applicable policy, rule, or law, and is consistent with your office or departmental policies and procedures related to such use, may be permitted. Faculty and Staff Users should consult with their supervisor as to the extent of permitted personal use of Saint Mary's IT Resources.

3.4.1.3.2.1.1 Use of College-Provided Mobile Computing Equipment

Faculty and Staff Users who are issued College-owned mobile computing equipment must also abide by the *Saint Mary's College of California Policy for College-Provided Mobile Computing Equipment.*

3.4.1.3.2.2 Students

Saint Mary's recognizes that access to, and use of, IT resources contributes to an individual's personal and intellectual development. Therefore, student Users may use IT resources for both academic and personal use. However, in an effort to allocate IT resources fairly, Users engaged in personal activities that place an undue burden on IT resources may be asked to reduce or discontinue such use. Saint Mary's may impose limits if the User does not voluntarily reduce or discontinue the burdensome activity upon such a request

3.4.1.3.2.3 Accounts and Passwords

Members of the Saint Mary's community, including Trustees, faculty, staff, current students, resident Brothers of the Christian Schools, and temporary employees are qualified for and will be issued a Saint Mary's network account (Account). Each Account will be issued with a unique user name and secret password, which should be immediately changed by the user to a strong password (see *Saint Mary's College of California Password Policy*). This user name and password will be required when authenticated access to Saint Mary's IT resources is necessary. Visitors to campus are limited to the use of the "Guest" wireless network, which does not require an account for access.

3.4.1.3.2.4 Attachment and Use of Privately-owned Computing Equipment

Users and Guests who attach their own (privately-owned) computing equipment to the Saint Mary's network must also comply with the *Saint Mary's College of California Policy Governing the Attachment and Use of Personally-owned Computing Equipment on the Saint Mary's Network.*

3.4.1.3.3 Information Security.

Users of Saint Mary's IT resources must comply with all provisions of the *Saint Mary's College of California Institutional Information Security Policy* that apply to the particular role of the User as defined in the Policy.

3.4.1.4 ELECTRONIC MAIL (E-MAIL)

3.4.1.4.1 General Information

Every network Account comes with an individually assigned e-mail account on the Saint Mary's Google Apps for Education domain (G-mail). Organizational email accounts not tied to an individual account are available by request to IT Services. Members of the Saint Mary's community are strongly encouraged to use the same personal and professional courtesies and considerations in E-mail as they would in other forms of communication at Saint Mary's.

3.4.1.4.2 Disclaimer

Saint Mary's IT Services is not the arbiter of the contents of E-mail, and is not technologically capable of completely protecting Users from receiving E-mail that the Users may find offensive. There is no guarantee that E-mail messages received by users of the College's email service are in fact sent by the purported sender. Furthermore, E-mail that is forwarded could be modified by persons other than the original sender.

3.4.1.4.3 Ownership

College E-mail addresses are the property of Saint Mary's College of California, and are intended for business purposes. (E-mail accounts issued to students are intended for both personal and educational purposes. Therefore, though Saint Mary's retains ownership of the email address, it claims no ownership or interest in the contents of the account; however, the account contents are visible to Saint Mary's.) Electronic mail sent to/from a College e-mail address, whether or not created or stored on Saint Mary's IT resources, constitute a College record subject to review and disclosure by Saint Mary's at its discretion. For reasons of security, business continuity and legal compliance, Saint Mary's employees must use their individual or departmental Saint Mary's e-mail account, rather than any other personal or business e-mail account, for all Saint Mary's business communications that utilize electronic mail.

3.4.1.4.4 Representations

E-mail Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Saint Mary's or any unit of Saint Mary's unless explicitly authorized to do so by the appropriate College authority. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not speaking on behalf of Saint Mary's. An appropriate disclaimer is: "These statements are my own, not those of Saint Mary's College of California, its Board of Trustees, or its Regents."

3.4.1.4.5 Lists and Aliases

Saint Mary's maintains e-mail lists and aliases to enhance communication among the Saint Mary's community. Certain lists are used for critical communication and are accessible only by members of the President's Cabinet and certain other emergency managers. Other lists may be created, as necessary, by Users working with their appropriate supervisor and IT Services. Users who participate in e-mail lists are expected to exercise good judgment and courtesy when posting to lists.

3.4.1.5 POLICIES RELATED TO THE USE OF IT RESOURCES

3.4.1.5.1. Management of Information Technology Resources

All Saint Mary's-owned computing equipment is managed by IT Services. Management includes the installation and maintenance of all application and operating system software. This may also include the installation of various software clients that aid in managing Saint Mary's owned computing equipment. No employee is permitted to evade or compromise this management or the capability of management, including the changing of administrative passwords or rights, nor does the granting of administrative rights on any Saint Mary's owned computer to a faculty or staff member confer the right to remove or alter any method of remote or local management by IT Services.

3.4.1.5.1.1 Adding Servers, Specialized Hardware and Applications

Employees and departments seeking specialized implementation of hardware or software applications in support of business-related objectives must follow the Project Proposal process of the TPPC (Technology Planning and Policy Committee) for approval and implementation (see *http://www.stmarys-ca.edu/provost-vice-president-for-academic-affairs/technology-planning-and-policy-committee* for more information). Lacking this review, specialized hardware and/or software that has been appropriated and/or attached to the Saint Mary's network may be immediately removed from Saint Mary's IT resources, or remotely disabled, by IT Services. Saint Mary's is not responsible for any lost data due any such action.

3.4.1.5.2 Archiving and Retention

Electronic Information, including E-mail, is backed up to assure system integrity, availability and reliability. Archived backups only exist in relation to need, based on legal or audit requirements, such as those made by the College's independent auditors. Under some circumstances, Saint Mary's could be required to disclose to outside parties certain electronic records, including but not limited to E-mail, web pages, or other electronic data archived by Saint Mary's. Saint Mary's may itself access or disclose User Electronic Information to law-enforcement agencies or other entities, consistent with this Policy and all applicable laws, court orders and rules of evidence requiring such disclosure.

3.4.1.5.2.1 Faculty and Staff Back-up of College documents and data

In order for the College to properly protect College business documents and data that reside on the computing devices used by employees of the College, employees must store or backup any such business documents and data files in their Saint Mary's Google Drive,

or on secure internal file servers. This method should be used for the proper and secure retention of electronic business documents and data.

3.4.1.5.3 Computer Labs and Computers for Library Use

Computer laboratories and Library general use computers maintained by Saint Mary's are resources installed by the College to promote scholarship and learning for all students. Accidental or intentional disruption of Computer laboratories and Library computer areas will deprive others of access to these important IT resources. Users of the computer labs and the Library general use computers shall obey the instructions of lab supervisors and other College employees. Behavior that is disruptive to other users of the facility is prohibited. Such behavior might include, but is not limited to, eating, drinking, making excessive noise, using aggressive or abusive language, or playing games.

3.4.1.5.3.1 Library and Lab User Courtesy

Users are responsible for leaving computers and workspace in laboratories and the Library clean and ready for the next User. This requires each User to close all open applications, log out of any attached servers, and remove personal items (including portable media and printouts) from the computer and workspace. Use of laboratory computers that are logged in under an Account other than one's own is prohibited.

3.4.1.5.4 Privacy and Discovery of Policy Violations during Routine Maintenance

Saint Mary's is committed to maintaining the privacy of all Users within the parameters of the *Saint Mary's College Institutional Information Security Policy*. However, Users should be aware that IT Services staff routinely monitor routing and other information related to data traffic across the Saint Mary's network, to evaluate issues such as volume of traffic, security breaches and the general use of system resources, and may detect policy violations during the normal course of this work.

3.4.1.6 PROHIBITED ACTIVITIES REALTED TO TECHNOLOGY USE

3.4.1.6.1 General

Users are subject to all Federal, State and local laws and College policies applicable to User conduct, including not only those laws and regulations that are specific to computers and networks but also those that may apply generally to personal conduct. Misuse of computing, networking, or information resources may interfere with the normal business of the College and can result in disciplinary action, loss of computing privileges, and/or legal action.

3.4.1.6.2 Examples

Examples of misuse and prohibited conduct include, but are not limited to, the activities in the following list. Since it is impossible for Saint Mary's to anticipate and thus give examples of every possible violation of this Policy, other applicable policies, or law, it is incumbent upon each User to consider the consequences of his/her own actions. To the extent that a violation of this Policy is also a violation of any Federal, State, or local law, Saint Mary's will encourage full enforcement of such laws by the appropriate public entity.

1. Reproducing, distributing or displaying copyrighted materials without prior permission of the copyright owner. This includes text, images, photographs, music files, sound effects, and other legally protected works.
2. Using an Account credentials that you are not authorized/assigned to use.
3. Sharing the password for your Account.
4. Using IT resources to harass others, or to create, store, or transmit libelous or obscene materials.

5. Sending chain, spam or any other junk email, disseminating mass email without the permission of the appropriate College authority, or intentionally creating/distributing email that contains malware or phishing attempts.
6. Using Saint Mary's IT resources to gain unauthorized access to any computer system. This includes the use of any network monitoring software or any other software that is used to assist in the compromising of a computer system or User Account.
7. Knowingly performing an act that will interfere with the normal operation of third party computers, peripherals, networks, or any Saint Mary's IT resource.
8. Knowingly running or installing on any computer system or network, or giving to another person, a program intended to damage or to place files on another Users' Account or system without their knowledge.
9. Using applications that inhibit or interfere with the use of the network by others, intentionally or not.
10. Attempting to circumvent data protection schemes or uncover security loopholes.
11. Violating terms of applicable software licensing agreements.
12. Masking the identity of an Account or machine, or using a false identity.
13. Using Saint Mary's IT resources to post materials on web sites. blogs, social media or electronic bulletin boards that violate existing laws, Saint Mary's codes of conduct, or any other Saint Mary's Policy applicable to the User.
14. Attempting to monitor or tamper with another person's electronic communications, or reading, copying, changing, or deleting another person's files or software without the explicit permission of the owner; capturing passwords or data on the network or Internet not meant for you.
15. Using IT resources for personal or political gain, including running a business for profit or non-profit purposes, promoting and selling products and services, commercial advertising, or political campaigning.
16. Registering a Saint Mary's IP address with any other domain name (i.e., www. name.com).
17. Providing a pass-through site or gateway that would give access to unauthorized persons to campus hosts and other Saint Mary's IT resources.

3.4.1.7 ENFORCEMENT OF TECHONOLOGY USE POLICY

3.4.1.7.1 Revocation of Privilege and Disciplinary Action

Saint Mary's reserves the right to limit or deny access to its IT resources when any Saint Mary's policy or any applicable Federal, State, or local laws are violated, or when Saint Mary's receives notice or believes that there is a violation by a User. Prior notice of such actions is not necessary. IT Services will notify the User of the violation and of any action as soon as is practicable under the circumstances. Further disciplinary action may be taken by the College as well. Third Party Users and other individuals who are subject to this Policy but might not be subject to any other Saint Mary's policy or disciplinary process (e.g., library patrons and Campus visitors), may lose the privilege to use Saint Mary's IT resources for violating this Policy, and, depending on the seriousness of the violation, may be banned from entering College property.

3.4.1.7.2 Reporting

If a User suspects that a particular behavior is in violation of this Policy, he or she should contact the ITS Service Desk.

3.4.1.7.3 Violations of Law

When there is a violation of law, a User may face other serious consequences imposed by public authorities. Violations of law, if brought to Saint Mary's attention, may result in the

temporary or permanent termination of User's access to IT resources, and the User shall be referred to the appropriate party for disciplinary action.

3.4.1.7.4 Copyright Infringement

In cases of alleged copyright infringement, Saint Mary's will comply with the Digital Millennium Copyright Act (the "DMCA"). In accordance with the DMCA, (17 U.S.C. § 512), upon receipt of proper notification by a copyright owner of an alleged copyright infringement, Saint Mary's will expeditiously take all appropriate and required actions, including but not limited to, the removal or disabling of access to the allegedly infringing material.

3.4.2 POLICY GOVERNING THE ATTACHMENT AND USE OF PERSONALLY OWNED COMPUTING EQUIPMENT ON THE SAINT MARY'S NETWORK (Bring Your Own Device)

3.4.2.1 General

The Saint Mary's College (Saint Mary's) Data network is a shared, finite resource installed by the College to promote scholarship and learning for all members of the College Community. The attachment of personally-owned computing equipment to the Saint Mary's network has the potential to disrupt it, if operated improperly, depriving others of access to the College's Information Technology resources. Persons attaching computing devices to the College's Saint Mary's network must comply with all portions of the *Saint Mary's College of California Technology Use Policy*. Additionally, Users who attach personally-owned computing equipment, including PC's, tablets, cell phones and any other computing or network-enabled device, to the Saint Mary's network are bound by the following specific policies:

3.4.2.2 Responsibility

Users are responsible for all traffic originating from their computing equipment, regardless of whether or not they generated it on purpose.

3.4.2.2.1 College Support for Personally-owned Computing Equipment

Due to resource limits, Saint Mary's cannot provide support for personally-owned computing equipment or software beyond assistance in securely accessing the Saint Mary's network and IT resources. The level of access allowed will be determined by the academic and/or business requirements of the individual's role at the College.

3.4.2.3 Installation of College-owned software

In all cases where licensing agreements prohibit it, Saint Mary's cannot provide or install software licensed to the College on any non-Saint Mary's-owned computing equipment.

3.4.2.4 Network Addresses

Network addresses on the Saint Mary's network are assigned by network DHCP servers. All personal computing devices connected to the Saint Mary's networks must be configured to use DHCP to obtain their IP network address and configuration settings. Static addresses are not allowed. Any computing device found out of compliance with this provision will be disconnected.

3.4.2.5 Routers and Servers

No personal routers, servers or wireless access points are permitted to be attached to the Saint Mary's network. Any devices that provide such services will be immediately disconnected from the campus network upon discovery.

3.4.2.6 Traffic Limits

It may not be feasible to provide unlimited connectivity for systems and/or applications that are not strictly serving the College's missions. Because of this possibility, IT Services may limit network usage of personal systems or non-supported applications. This may be implemented through bandwidth caps, restriction or blocking of services, or by other means.

3.4.2.7 Security

Users are responsible for the security and integrity of their own systems. If a system has been "hacked" or otherwise compromised, IT Services may disconnect it to prevent it from interfering with the proper operation of the network. In such a case, the User is responsible for removing all malware, and the User must present evidence to IT Services that their equipment is clean before the system can be reconnected Typical acceptable evidence would be a work order from an established repair facility attesting to the work performed by them to remove the malware, and final test results.

3.4.2.7.1 Virus Protection and Patches

All computers attached to the Saint Mary's network are required to have an effective commercial virus protection program installed, actively running and currently updated to include the most recent virus protection offered by the manufacturer. Additionally, User computers connected to Saint Mary's networks must have installed all operating system and application "patches" provided by the manufacturers to fix potential security risks in their software. Computing systems that use obsolete operating systems or applications that are no longer supported by the manufacturer cannot comply with the above requirement and should not be connected to the Saint Mary's network. Systems that are found to be out of compliance with this provision may be blocked or disconnected by IT Services.

3.4. 2.7.2 Sensitive College Data

Legally protected and sensitive data as defined by the *Saint Mary's College of California Institutional Information Security Policy* may not be stored on personal computing devices not owned by the College. Additionally, Users must configure any mail client used on a personal computing device for viewing Saint Mary's email so that messages stay on the server and are not permanently moved to the personal computing device (no POP clients allowed).

3.4.2.8 Abuse

Systems found to be running programs that disrupt network services or attack data equipment (including Denial of Service attacks) on or outside the campus network will be disconnected or blocked immediately by IT Services. Depending upon the circumstances of the incident, disciplinary action may be taken by the College.

3.4.2.8.1 Reconnaissance

Use of any type of "packet sniffing," port mapping or other similar reconnaissance programs or devices by Users is strictly prohibited. Users may run a packet sniffer in non-promiscuous mode (you may sniff your own machine's packets only)

3.4.3 POLICY FOR COLLEGE-PROVIDED MOBILE COMPUTING

(Note: The Policy governing the use of College-funded Mobile Telephone equipment is located on the Business Office pages on www.stmarys-ca.edu, under Accounts Payable, and is entitled *Cell Phone Policy, Procedures and Form*)

3.4.3.1 General

Mobile computing equipment belonging to Saint Mary's College of California (Saint Mary's), such as laptop or tablet computers, may be issued to Faculty and Staff Users as needed for the requirements of the official academic or administrative tasks they perform. The equipment shall remain in the possession of the User until the end of the term specified in the *Mobile Computing Equipment Lending Agreement*, which will be provided to the User when the equipment is delivered, and must be signed by the User before taking possession of the equipment. This equipment should be used primarily for College-related work. Excessive use for non-College related activities is not appropriate. Any personal or private communications, data or information that a User may store on Saint Mary's mobile computing equipment will be exposed to Saint Mary's during routine maintenance and repair (see 3.4.3.3 below). Additionally, Saint Mary's shall not be responsible for the loss or disclosure of any personal data, information or communications maintained by a User on Saint Mary's mobile computing equipment.

3.4.3.2 Software not provided by the College

Mobile computing equipment must be used in compliance with all applicable copyright laws. This means that only properly licensed software may be installed on College-owned equipment. The User will ensure that any software he/she installs on College-owned mobile computing equipment is covered by licenses owned by Saint Mary's, or has licenses that permit the installation and use of the software on College-owned equipment, or is open-sourced (free, without restriction). The User will also maintain records of the licenses and purchase information of any such software so that it can be produced, if required, during a copyright audit. In addition, due to resource limitations, IT Services cannot provide support for any non-College provided software that a User installs on College-owned Mobile computing equipment, other than for its removal.

3.4.3.2.1 Prohibited Software

There are certain classes of non-College provided software that Users are not allowed to install on any mobile computing equipment owned by Saint Mary's. However, if a specific institutional or business need that can only be fulfilled by the use of prohibited software can be documented by the User, an exception to this provision may be obtained after approval by the appropriate subcommittee of the Technology Planning and Policy Committee (TPPC).

Peer to Peer (P2P) File Sharing Software, such as BitTorrent, can be easily mis-configured, and can expose College assets and information to risk and illegal copying by others. P2P software may not be installed on College-owned computing equipment, unless an exception as outlined above is obtained prior to installation.

3.4.3.3 Maintenance and Repair

Saint Mary's reserves the right to recall the provided equipment for inventory, upgrades, repair, replacement, or for any other reason, and the User will return the equipment in a timely fashion when recalled. Efforts will be made to minimize the inconvenience of a recall to the User. College-owned equipment shall not be repaired or altered in any way except by IT Services personnel. The User shall notify the ITS Service Desk promptly when any repair is needed.

3.4.3.4 Protection of Sensitive and Legally Protected Data on Mobile Computing Equipment:

Legally protected and sensitive data may not be stored on a laptop hard drive or portable digital media in unencrypted form. Such data should normally be stored on College file servers, and Mobile equipment Users should download the data to their computing device only when needed, and then upload changes and remove the data from the mobile computing device when the work is finished. When compelled by circumstance to use portable media (thumb drive, SD card, etc.) to transport or temporarily store legally protected or sensitive data, Users should employ only encrypted portable media and carry or store it separately from the mobile device.

3.4.3.5 Damage and Loss

The User must report any damage or loss of the provided equipment to IT Services immediately. Stolen equipment must also be immediately reported to Public Safety and to the Police agency with jurisdiction over the location where the theft occurred.

3.4.3.5.1 Responsibility

Damage to College-owned equipment or loss caused by neglect or carelessness may cause all or a part of the repair or replacement costs to be charged to the User. Saint Mary's may consider a failure by the User to report loss or damage in a timely fashion as evidence of the User's responsibility for such loss or damage. Failure by the User to abide by this policy may result in the revocation of all borrowing privileges to mobile equipment owned by Saint Mary's.

3.4.3.5.2 Loss of Sensitive Information

Users must report the loss or theft of a laptop, tablet, portable digital media or any other device containing legally protected and sensitive information as defined by the *Saint Mary's College Institutional Information Security Policy*, or any other College Security Policy, immediately, to the Information Security Officer (ISO) and to their supervisor or department chair.

3.4.4 PASSWORD POLICY

3.4.4.1 General

The issuance of a User password or other means of authenticated access to College systems is intended to ensure the appropriate security of College data. It does not guarantee complete privacy for users' personal information or sanction improper use of College equipment, facilities or data, and is intended to prevent unauthorized third party access to any account information. User should be aware that passwords or other means of authenticated access does not prevent Saint Mary's from viewing account content

3.4.4.2 Password Minimum Requirements

In order to protect the security of the College's systems and data, all Users are required to use strong passwords. Strong passwords are those which are at least eight characters long (ten or more is recommended for better security), containing a mix of both alphanumeric and non-alphanumeric characters (e.g. #, %, ^, &, etc.). Obvious or predictable words that can be guessed, like the names of people, places or commonly used words, or information that can be easily found out, like the name of a pet, or an address or birthday, should be avoided.

3.4.4.2.1 Password Maintenance

Password change is currently required of all Faculty and Staff Users, and for all organizational (fictitious) accounts, once every year for all systems. Students are encouraged to do the same, but are not required to. Any password used for access to Saint Mary's IT resources should be unique and not used for access to any other site or application.

3.4.4.3 Security

Passwords used for access to Saint Mary's IT resources should never be revealed to anyone. Appropriate measures must be taken by all Users to protect their Saint Mary's password. If a User suspects that his or her password has been revealed to an unauthorized person, the User should change it immediately. Violations of this provision may result in appropriate disciplinary action.

3.4.4.3.1 Exceptions

Passwords may be revealed under certain circumstances to:

- Law-enforcement agencies and courts requesting information under court orders and rules of evidence that require disclosure.
- Supervisors (Employees only)

3.4.4.4 Enforcement

This password policy may be enforced by automated systems that will not accept weak passwords or allow users to log in without changing their passwords if they have not done so within the stated time intervals.

3.4.5 WEB AND BLOG USE POLICY

3.4.5.1 General

Web pages and blogs, authored by the students, faculty and staff of Saint Mary's College of California (Saint Mary's), are a primary means of communication within the larger College community, and with the public. They are critical in presenting the mission and culture of Saint Mary's College to the outside world, and are also used internally for teaching and learning, and for business processes. The use of web pages and blogs that are a part of, or use, Saint Mary's IT resources must comply with the following policy.

3.4.5.2 Saint Mary's Official Web Pages

The official Saint Mary's web pages are official publications of the College. Official pages include content related to academic programs, administrative and student support offices, programs and services, official College programs and intercollegiate athletic teams and activities.

3.4.5.2.1 Official Content

Original text, photographs and graphics appearing on the official pages of Saint Mary's web site are copyrighted by Saint Mary's and may not be reproduced or altered without written permission from Saint Mary's. Content posted to the official pages of Saint Mary's website that are not original content must bear the copyright, or other form of acknowledgement to the copyright holder, unless such content is already a part of the public domain.

3.4.5.2.2 Responsibility

The Office of College Communications provides the overall management of the official College web pages. They are responsible for operational practices and policies, and for ensuring the presentation of a consistent image within the College's publication standards.

IT Services is responsible for maintenance and administration of the web servers, including contract arrangements for cloud provisioning of these services, if employed.

Each Department or Student Organization with web pages has the responsibility to maintain its own pages by at least one annual review. Each department and Student Organization is responsible for the editorial content of these pages. IT Services provides support to Departments and Student Organizations in the maintenance of their web pages.

3.4.5.2.3 Domain Names

All domain names used in support of official College departments, programs or activities must be registered by the College, with the College as the official owner of the name, and with IT Services as the Administrative Contact. Such domain names should also be registered with the College's DNS servers as authoritative. No individual or group may seek to register a domain name that incorporates or otherwise mimics a name, nick-name or mark of Saint Mary's.

3.4.5.3 Personal Web Pages and Blogs

Personal web pages and blogs provide an individual with an opportunity to share personal interests and information to the Campus Community, and the world at large via the Internet. SMC Google Sites are provided for personal web space, and SMC Google Blogger is provided for personal blogs. Both are available to a User through their Saint Mary's G-Mail account

3.4.5.3.1 Conduct

Saint Mary's expects Users to maintain basic standards of decency, courtesy, civility, and maturity when creating or posting to personal pages and blogs using Saint Mary's IT resources. Any User not wishing to comply with this guideline has the option of using a personal Google account or finding an independent Internet service provider to host that User's personal web pages or blogs, at the User's own expense.

3.4.5.3.2 Content

Information posted or made available on a User's personal web or blog pages must be the original work of the User, and must not be the intellectual property or copyrighted work of other persons or entities, unless appropriate permission has been obtained by the User. Personal pages and blogs should not carry any Saint Mary's logo, the name, or any abbreviation of, Saint Mary's College of California in such a manner as to suggest that the page or blog is affiliated with Saint Mary's in any way. This does not apply to a factual statement regarding Saint Mary's being the User's place of employ or place of study.

Users must abide by Saint Mary's code of conduct when publishing content on a User's personal web or blog pages, including but not limited to, refraining from engaging in abuse, threats, intimidation, harassment, coercion, indecent or obscene conduct, or violations of law. Users shall refrain from publishing statements, images, photos or audio/video clips that have the observable effect of unreasonably interfering with a person's ability to work or to participate in the educational benefits at Saint Mary's. Users are prohibited from posting any content that includes intimate/sexual images, photos or videos without the consent of the person depicted in the image, photo or video. Persons who believe content has been posted on any Saint Mary's site or blog that violates this policy may request removal by sending an email message with the details to itshelp@stmarys-ca.edu.

3.4.5.3.3 Disclaimer

Saint Mary's accepts no responsibility for the content of personal home pages or blogs. Saint Mary's College does not pre-approve, monitor, or exert editorial control over

personal pages or blogs. Nonetheless, personal web sites and blogs must conform to all terms and conditions of this Policy.

THE PERSONAL WEB PAGES OR BLOGS OF SAINT MARY'S COLLEGE STUDENTS, STAFF AND FACULTY DO NOT IN ANY WAY CONSTITUTE OFFICIAL COLLEGE CONTENT. THE VIEWS AND OPINIONS EXPRESSED IN THE PERSONAL PAGES OR BLOGS ARE STRICTLY THOSE OF THE AUTHORS, AND COMMENTS ON THE CONTENTS OF THOSE PAGES OR BLOGS SHOULD BE DIRECTED TO THE PAGE OR BLOG AUTHORS.

3.4.5.4 Violations

See Section 3.4.1.7