SAINT MARY'S COLLEGE OF CALIFORNIA
GENERAL POLICIES GOVERNING THE USE OF INFORMATION TECHNOLOGY

Revised 2017

1.0 IT Policy Governance

This and other Related IT Policies (listed below under "Related Policies") are subject to amendment or revision as appropriate by approval of the President's Cabinet.

2.0 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.

3.0 USING INFORMATION TECHNOLOGY RESOURCES

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.[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.

3.2.1 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.

3.2.1.1 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.*

---

[1] 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.

3.2.2 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

3.2.3 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.

3.2.4 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.*

3.3 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.

4.0 ELECTRONIC MAIL (E-MAIL)

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.

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.

4.3 Ownership

College E-mail addresses are the property of Saint Mary's College of California, and are intended for business purposes.[2] 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.

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."

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.

5.0 POLICIES RELATED TO THE USE OF IT RESOURCES

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.

---

[2] 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.

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.

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.

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.

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.

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.

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.

6.0 PROHIBITED ACTIVITIES

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.

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..

7.0 ENFORCEMENT

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.

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.

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.

7.3.1 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.

Related Policies

Saint Mary's College of California Technology Use Policy
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
Saint Mary's College of California Institutional Information Security Policy