

# St. MARY'S COLLEGE OF CA TECHNOLOGY USE POLICY

(May 07, 2009)

## 1.0 INTRODUCTION

Saint Mary's College of California ("Saint Mary's") recognizes the educational value and societal significance of **Electronic Information** and **Computing Resources** systems. Therefore, Saint Mary's supports students, Christian Brothers, faculty, and staff by providing access to those valuable electronic resources.

Saint Mary's is a non-profit public benefit corporation dedicated to offering a Catholic, Lasallian, Liberal Arts education. To support the College's mission, Saint Mary's has developed a campus-wide computing system allowing its members to form an electronic link to the College and to the Internet.

This **Policy** presents guidelines for acceptable use of **Saint Mary's Computing Resources**. It serves as a reference for all persons using **Saint Mary's Computing Resources** or having a Saint Mary's E-mail or Internet access **Account**. This **Policy** supercedes all prior policies and guidelines governing the use of **Saint Mary's Computing Resources**.

The Saint Mary's community is encouraged to make innovative and effective use of its **Computing Resources** within a framework which provides standards for the quality and content of information, while requiring compliance with laws, as well as requiring compliance with Saint Mary's policies governing students, faculty, and staff.

This **Policy** seeks to ensure that Saint Mary's maintains a consistent and accurate image of itself while complying with moral and ethical standards. This **Policy** is subject to amendment or revision as appropriate.

## 2.0 DEFINITIONS

All defined terms shall appear in **Title Case** and **Bold Font** throughout this **Policy**.

**Account**: Special access to **Saint Mary's Computing Resources** with unique **User** identification provided by Saint Mary's College. This includes, but is not limited to, having a Saint Mary's E-mail **Account**, having access to networks operated or maintained by Saint Mary's, and/or having access to the Internet through **Saint Mary's Computing Resources**. Only **Users**, as defined in this **Policy**, may have an **Account**.

**Computing Resources**: any computer hardware, including but not limited to wiring and cabling, and/or software owned or licensed by Saint Mary's, any Saint Mary's computing

systems, or any service provided by Saint Mary's for access to the Internet. Also referred to as **Saint Mary's Computing Resources**.

**Electronic Information:** any information or data (e.g. - E-mail, word processing files, data entered on online forms, web pages, etc.) placed on **Saint Mary's Computing Resources**, whether through a Saint Mary's Computing Resource or through an individual's own computer or other personal electronic data storage device.

**CaTS:** Computer and Technology Services. The department at Saint Mary's primarily responsible for maintaining all **Computing Resources**.

**Policy:** This Technology Use **Policy**.

**Third Party User(s):** persons having access to **Saint Mary's Computing Resources** whom do not fall within the definition of **User(s)** and who therefore do not have an **Account** (e.g.- members of the public using **Computing Resources** in the library). Such persons are required to agree to, and abide by, the terms of this **Policy** when using **Computing Resources**.

**User(s):** Current Saint Mary's students, faculty, and other employees including third party contractors who have full time presence on campus and who need access for their official duties (e.g., Sodexo Marriott, Barnes and Noble etc.), trustees, regents and other members of official boards and committees as designated by the President, as well as Christian Brothers at Saint Mary's having access to Saint Mary's Computing Resources.

### **3.0 USING COMPUTING RESOURCES**

#### **3.1 General**

**Saint Mary's Computing Resources** can be used to host information maintained by a Department, an Office, a properly registered student club or organization, a board, or a committee. Any information used with **Saint Mary's Computing Resources** must adhere to all applicable laws and all Saint Mary's policies.

The use of **Computing Resources** shall be consistent with the mission of the College, College policy and must not violate laws or any College **Policy**. If a **User** has questions regarding the acceptability or appropriateness of a particular behavior while using **Saint Mary's Computing Resources**, he or she should contact the appropriate College official. For example, an issue regarding one student allegedly harassing another via a Computing Resource would be forwarded on to the Dean for Student Development and Leadership. Or, for example, an issue involving copyright infringement on a faculty or staff member's web site would be forwarded to the faculty or staff member's direct supervisor. Additionally, **CaTS** staff can help **Users** address technical and non-substantive legal issues. If **Users** have questions regarding copyright and trademark issues, fair use, or other legal matters; please refer to Saint Mary's General Counsel SMCnet Page located at (Address TBD) or contact Saint Mary's Office of General Counsel.

#### **3.2 Access**

**Computing Resources** are available to **Users** on campus as well as remotely through dial-in-modem connections, twenty-four hours a day, seven days per week. Technical support is limited to business hours and Saint Mary's may on occasion temporarily interrupt access of **Users** to conduct ordinary as well as extraordinary business and maintenance.

### **3.2.1 Faculty and Staff**

Use of **Computing Resources** is limited to that which is necessary as part of a **User's** duties and responsibilities in **User's** employment. Incidental or minimal personal use during a **User's** working hours where such use does not interfere with a **User's** performance, or does not violate any applicable **Policy**, rule, or law, may be permitted. Specific questions regarding personal use of **Computing Resources** during a **User's** working hours should be directed to the **User's** supervisor, Dean, department head, or vice president, as appropriate. Monitoring and control of personal use of **Computing Resources** during a **User's** workday is at the discretion of the person under whose direction the **User** works. A **User's** performance appraisal may take into account personal use and a supervisor may limit personal use as a condition of employment where appropriate.

Use of **Computing Resources** on **User's** own time is permitted to the extent that **Computing Resources** are available. **Users** needing to use **Computing Resources** for official Saint Mary's business, whether administrative or academic, shall always have precedence over any **User** using **Computing Resources** for personal matters. Therefore, **Users** engaged in personal activities may be asked to discontinue such use to free **Computing Resources** for **Users** needing to access Computer Resources for non-personal matters.

E-mail may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (1) directly or indirectly interfere with Saint Mary's operation of **Computing Resources**; (2) burden Saint Mary's with noticeable incremental cost; or (3) interfere with the **User's** employment or other obligations to Saint Mary's.

#### **3.2.1.1 Portable Computing and Telecommunications Equipment**

Portable computing and telecommunications equipment belonging to the College, such as laptop computers or cell phones, 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 portable [computing](#) or [telecommunication](#) equipment lending agreements, which must be signed by the **User**. Saint Mary's reserves the right to recall the equipment for inventory, upgrades, repair/replacement or for any other reason, and the **User** will return the equipment in a timely fashion if recalled. Efforts will be made to minimize the inconvenience of a recall to the **User**. This equipment shall not be repaired or altered in any way except by Computer and Technology Services or Telephone Services personnel. The **User** shall notify the appropriate (**CaTS** or Telephone) Help Desk promptly when either of these tasks are needed. The **User** must report any damage or loss of the equipment to **CaTS** or Telephone Services immediately. Stolen equipment must also be immediately reported to Public Safety and an Incident Report filed. Damage 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.

Portable computing and telecommunications equipment belonging to Saint Mary's should be used primarily for college-related work. Excessive use for non-College related activities is not appropriate, and, in the case of portable telephone equipment, the **User** may be charged for excessive personal calling if so deemed by the **User's** supervisor. Portable computing equipment must be used in compliance with all applicable copyright laws. This means that only properly licensed software may be installed on the equipment. The **User** will ensure that any licensed software installed on College owned portable computing equipment which is not covered by licenses owned by Saint Mary's, or are open-sourced (free, without restriction), have licenses that permit the installation and use of the software on college-owned equipment. 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. Please refer any questions on this requirement to the Director of **CaTS**.

Failure by the **User** to abide this policy may result in the loss of all **User** privileges of portable equipment owned by Saint Mary's.

### **3.2.1.2 Guidelines for Protection of Sensitive and Legally Protected Data on Portable Computing Equipment:**

- Legally protected and sensitive data may not be stored on a laptop hard drive or floppy drive in unencrypted form
- Legally protected and sensitive data must be stored on College file servers (e.g. FS1) , and laptop **Users** should download such data to their computers only on an as needed basis, and remove it from the computer when it is no longer needed
- Legally protected and sensitive data used with a laptop must be stored on a Flash Drive (“thumb drive”, “flash memory stick”) in an encrypted format, or on other media in encrypted format.
- Flash Drives containing legally protected or sensitive data must be stored separately from the laptop.
- Legally protected and sensitive data must not be stored on personal computers not owned and maintained by the College.
- **Users** must report the loss or theft of a laptop, flash drive or any other device containing legally protected and sensitive information immediately to the Chief Technology Officer, and to their supervisors or department chairs.

- Laptops must have current and active anti-virus and anti-spyware programs running at all times.

(Adopted 09-07-06 TAC)

### **3.2.1.3 Management of Computing Resources**

All Saint Mary's owned computing equipment is managed by **CaTS**. Management includes the installation and maintenance of all application and operating system software. This may 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 by, 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 **CaTS**.

(adopted 03-08-07 TAC)

### **3.2.1.4 Attachment and Use of personally-owned computing equipment on the Saint Mary's Network by Faculty, Staff and Authorized Third-Party Users**

All provisions of Section 6.0 (Residential and Wireless Networks – see below) also apply to the use of personally-owned computing equipment attached to any portion of the Saint Mary's Network by Faculty and Staff members, or by authorized Third-party **Users**. 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.

(adopted 03-08-07 TAC)

### **3.2.2 Students**

Saint Mary's recognizes that access to, and use of, **Computing Resources** contributes to an individual's personal and intellectual development. Therefore, student **Users** may use **Computing Resources** for both academic and personal use. However, in an effort to allocate **Computing Resources** fairly, **Users** engaged in personal activities that place an undue burden on **Computing Resources** may be asked to discontinue such use.

### **3.3 Accounts**

Generally, **Users** are issued an **Account** or **Accounts** at the beginning of his or her relationship with Saint Mary's to gain access to appropriate **Computing Resources**. However, if an individual qualifies for an **Account** but does not have an **Account**, one may be obtained by contacting **CaTS**.

[Follow link to request an Internet/E-mail Account](#)

#### **3.3.1 Passwords**

The issuance of a **user's** password or other means of access to College systems is intended to ensure the appropriate security of College data and information in the

systems. It does not guarantee complete privacy for **users'** personal information or sanction improper use of College equipment, facilities or data.

Saint Mary's may, and from time to time, shall monitor any and all aspects of College systems, including but not limited to logon sessions, E-mail use, Internet use, Intranet use, and other uses of **Saint Mary's Computing Resources** to determine if a user is acting in violation of Saint Mary's policies or rules.

In order to protect the security of the College's systems and data, **users** are required to use strong passwords, and to change them at appropriate intervals. Strong passwords are those which are at least eight characters long, containing both alphanumeric characters and non-alphanumeric characters (e.g. #, %, ^, &, etc.)

Appropriate change intervals are currently deemed to be at least once every 180 days for all systems.

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

(Revised 1-15-09 TAC)

### **3.4 Adding Computing Systems**

The College seeks to provide necessary resources to meet ' needs. However, individuals seeking to add their own computing systems to **Saint Mary's Computing Resources** must meet with their supervisor (i.e., manager, department chair, or Dean) for approval and then must meet with **CaTS** in order to determine whether **Computing Resources** exist to meet the need.

#### **3.4.1 Hardware and Software**

**CaTS** requests that **Users** refrain from installing/attaching unsupported hardware and/or software to **Computing Resources**. Upon the discovery of unauthorized hardware and/or software, including but not limited to unauthorized software, it will immediately be removed from **Saint Mary's Computing Resources** by **CaTS**. Saint Mary's is not responsible for any lost data due to such removal.

#### **3.4.2 Servers**

**CaTS** is responsible for the overall maintenance of **Saint Mary's Computing Resources**. An important part of this responsibility is to ensure the overall security of all **Computing Resources**. When computers and devices attached to the network run network services (i.e., web servers, file sharing, e-mail servers, etc.) these services "open" a computer to security risks. When one **Computing Resource** is compromised or "hacked" others on the network become easier to compromise.

Saint Mary's also recognizes the benefit that running these services may have to the educational purposes and business needs of the College. Therefore, **CaTS** strives to provide open and reliable access to these services for the whole College community. Under some circumstance, some non-student **Users** (individual student **Users** are not

permitted to run networks or servers) may need to run their own network services on their own machines. Student **Users** may not operate servers on the College's network, only sanctioned student groups are permitted to do so.

Use of networked servers attached to **Saint Mary's Computing Resources** by faculty and staff is subject to the terms and conditions of this **Policy**. The administrator of the attached system is responsible for all traffic that originates from that system. However, because **CaTS** is primarily responsible for all **Computing Resources** the following policies are also in effect:

Faculty and staff run servers on **Saint Mary's Computing Resources** shall be for the purpose of supporting the educational needs and business purposes of the College.

All servers must pass security audits conducted by **CaTS**.

Faculty and staff must register their servers annually with **CaTS**, using the form found at: [/technology/tcc/policy/server\\_registration.html](http://technology/tcc/policy/server_registration.html)

### **3.5 Archiving and Retention**

Saint Mary's record management policies do not distinguish among media. As such, electronic data and information, including but not limited to E-mail records, are subject to these policies, which include archiving (backing-up) **Electronic Information**. **Users' Electronic Information** is copied in the normal course of business when **Electronic Information** is archived. **Users of Computing Resources** should be aware that despite the sender and recipient having both discarded their copies of an electronic record, there may be retrievable back-up copies. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of **Electronic Information**. The practice and frequency of back-ups and the retention of back-up copies of **Electronic Information** vary from system to system.

**Users** should be aware that, during the performance of **CaTS's** duties, staff and other personnel need from time to time to observe certain transactional addressing information to ensure proper functioning of **Saint Mary's Computing Resources**, and on these and other occasions may see the contents of **Electronic Information**. Therefore, the security and confidentiality of E-mail and all other **Electronic Information** cannot be guaranteed

#### **3.5.1 Back-up of College documents and data**

In order for the College to properly back up College business documents and data, employees of the College who use Windows-based computing equipment must store any such business documents and data files in the "My Documents" directory on their local computer. This is the only directory that is synchronized with network backup systems, and must be used for the proper and secure retention of electronic business documents and data. (Apple and Linux desktop requirements to follow in a future revision).  
(adopted 03-08-07 TAC)

### **3.6 Maintenance**

Any **Electronic Information**, which contains incorrect or out-dated information may be removed until corrected. **CaTS** will attempt to provide reasonable notice of the removal of **Electronic Information**, but reserves the right to act without notice if the situation warrants.

## **4.0 WEB PAGES**

### **4.1 Introduction and Universal Policy: Applicable to all Web Pages**

Saint Mary's College recognizes the educational value of the exchange of **Electronic Information**. Saint Mary's web pages provide the College with the opportunity to share itself, its mission, and its culture over the Internet. Therefore, it supports students, faculty, staff, and other employees in the electronic publication of information and collaborations.

Information posted or made available on **Users'** web pages must be the original work of **Users** and must not be the intellectual property or copyrighted work of other persons or entities, unless appropriate permission has been obtained by the **User**.

Web pages that represent official information about the College are clearly different from those pages that are solely intended for the educational and personal use of **Users**. The College is sensitive to the desire of **Users** to express their ideas on **User Web** pages. Therefore, the College has set forth the following guidelines.

### **4.2 Saint Mary's Official Web Pages**

#### **4.2.1 Purpose**

The Official College pages communicate with internal as well as broad external audiences, including prospective students, alumni, constituents and the general public. Therefore, the appropriate supervisor (e.g., manager, department chair, or Dean), in collaboration with the Webmaster, shall review and approve the content of all official web pages. (Note: the appropriate supervisor for registered student clubs and organizations is the Director of Student Activities and Leadership Programs.) As well as adhering to this **Policy**, these pages must conform to aesthetic standards (e.g. - font, symbols, and other user interface elements) as well as style guidelines. These standards are located at: (Address TBD)

#### **4.2.2 Official Content**

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.

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.

#### **4.2.3 Responsibility**

The Webmaster provides for the overall management of the web pages, operational practices and policies and for the presentation of a consistent image within the College's publication standards. **CaTS** is responsible for maintenance of web servers.

#### **4.3 Departmental and Student Organization Web Pages**

Official Departmental and Student Organization web pages provide individual groups within the College an opportunity to share specialized interests and information over **Saint Mary's Computing Resources** generally (e.g. - SMCnet), as well as over the Internet. Departments and Student Organization pages bear official ties to the College and therefore must conform to the requirements found in the section (above) pertaining to official web pages. Included in Departmental pages are any pages developed by faculty and staff to support the mission and business of the College.

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

To obtain guidelines and support for maintaining web pages see the following:  
(<http://www.stmarys-ca.edu/news-and-events/college-communications/guidelines/web.html>)

##### **4.3.1 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 Computer and Technology Services as the Administrative Contact. Such domain names should also be registered with the College's DNS server as the authoritative DNS server.

#### **4.4 Personal Home Pages**

Personal home pages provide an individual with an opportunity to share personal interests and information to friends, family, and the world at large via the Internet. Personal pages concentrate primarily on personal information and non-professional interests of a **User**. **Users** are afforded extended creative license in structuring these pages. However, Saint Mary's expects **Users** to maintain basic standards of decency, courtesy, civility, and maturity when creating personal pages using **Saint Mary's Computing Resources** or when posting personal web pages on Saint Mary's servers. Any **User** not wishing to comply with this guideline has the option of finding an independent Internet service provider to host that **User's** personal home pages, at the **User's** own expense.

For system administration and general disclosure purposes, each personal web page shall contain contact information for the person responsible for maintenance of the web page. Each page should also contain the date on which it was last updated. This information may be provided as text in the document or as a link. This encourages the page manager to keep it current thus protecting the viewer from unknowingly reading outdated information.

Saint Mary's accepts no responsibility for the content of those personal home pages. Saint Mary's College does not pre-approve, monitor, or exert editorial control over personal pages. Nonetheless, personal web sites must conform to all terms and conditions of this **Policy**.

Personal pages 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 is affiliated with Saint Mary's in any way. This does not include a factual statement regarding Saint Mary's being the **User's** web service provider, place of employ or place of study.

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

If activities or content is discovered that may constitute a violation of this **Policy** or is suspected of violating any law, Saint Mary's shall investigate the situation according to the applicable procedure.

Link to Procedure for suspected **Policy** violations or suspected violations of law. (TBD)

**CaTS** provides for the overall management of the personal web servers. The Webmaster processes requests for personal web space. Requests for this web space may be made at the following address: [/college\\_services/its/web\\_services/forms/personal\\_space.html](http://college_services/its/web_services/forms/personal_space.html).

## **5.0 ELECTRONIC MAIL (E-MAIL)**

### **5.1 General Information: Security and Privacy**

The nature of E-mail makes it less private than **Users** may anticipate. For example, E-mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or "listserver" intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an E-mail record from a computer or an **Account**, it may persist on backup facilities. Saint Mary's cannot protect **Users** against such eventualities.

Saint Mary's is not the arbiter of the contents of E-mail. Saint Mary's is not technologically capable of protecting **Users** from receiving E-mail that the **Users** may find offensive. 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, in addition to abiding by the terms of this **Policy**.

There is no guarantee that E-mail sent through **Computing Resources** are in fact sent by the purported sender, since it is relatively straightforward, although a violation of this **Policy**, for senders to disguise their identity. Furthermore, E-mail that is forwarded could be modified by persons other than the original sender.

College E-mail addresses are owned by Saint Mary's. Electronic mail, whether or not created or stored on **Saint Mary's Computing Resources**, may constitute a College record subject to disclosure under certain laws.

**Electronic Information**, including E-mail, is backed up to assure system integrity and reliability, not to provide for future retrieval, although backing up may at times serve the latter purpose incidentally. 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 requiring such disclosure.

## **5.2 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 appropriately explicitly authorized (explicitly or implicitly) to do so. 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."

## **5.3 Lists and Aliases**

Saint Mary's maintains e-mail lists and aliases to enhance the facilitation of communication among the Saint Mary's community, as well as with parties outside of the College community. Certain lists are for critical communication and are accessible only by President and Vice Presidents. Other lists may be created, as necessary, by **Users** working with their appropriate academic or administrative supervisor and **CaTS**. **Users** who participate in e-mail lists are encouraged to exercise good judgement when posting to lists. **Users** posting to a list are also encouraged to be aware of the intended and expressed purpose of the list, as well as the other members of the list.

## **6.0 RESIDENTIAL AND WIRELESS NETWORKS**

The Residential and Wireless Networks are shared, finite resources installed by the College to promote scholarship and learning for all students. Accidental or intentional disruption of the residential or wireless networks will deprive others of access to this Computing Resource. Persons attaching computers to the College's residence hall or wireless networks must comply with all other portions of this **Policy**. Additionally, the administrators of the residential and wireless networks have the following specific policies:

## **6.1 Responsibility**

**Users** are responsible for all traffic originating from their machine, regardless of whether they generated it or realize that they have violated any specific policies. In most cases, unintentional violations will result in a temporary loss of network access pending the resolution of the problem.

## **6.2 Identification**

All machines connected to the residential or wireless network must be authorized by **CaTS** before use. This is done by accessing the authorization web page upon opening a web browser and entering the **User's Internet Account** username and password. Network access is not allowed without following this procedure each time the machine is used on the residential network.

## **6.3 Network Addresses**

Network addresses on the residential or wireless networks are assigned by the residential network DHCP server. All machines connected to the residential or wireless networks must be configured to use DHCP to obtain their IP network address. Static addresses are not allowed. Any machine found with an address not assigned by the residential or wireless networks' DHCP server will be disconnected.

ResNet subscribers may not register a domain name or alias with an outside provider that points to a machine on the Residential Network.

## **6.4 Routers and Servers**

No routers, servers or wireless access points are permitted to be attached to the SMC residential or wireless networks. Any devices that provide such services will be immediately disconnected from the campus network. Ethernet hubs, which allow multiple devices to be connected to a single network jack, are not routers and are allowed.

Most computer operating systems do not provide routing functionality and are by default safe to attach to the network. Some operating systems such as Windows NT, Windows 2000, as well as most Unix and Linux implementations have the ability to provide routing functionality. If a **User** uses one of these operating systems, the **User** must make sure that all routing functionality is disabled. These operating systems also frequently provide server functionality by default. **Users** must make sure that all server services are disabled before attaching such a machine to the residential or wireless networks. Routing and some network services, such as DHCP servers can disrupt the ability of others to use the residential or wireless networks. If routers or servers are found to be operating, they will be immediately disconnected. All types of servers are prohibited, including but not limited to, web servers, FTP servers, IRC/chat servers, streaming audio/video servers, web cameras, DHCP servers, mail servers, anonymous remailers, and file servers. This includes Windows and MacOS personal file sharing services.

## **6.5 Network Traffic**

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

It may not be feasible to provide unlimited connectivity for systems that are not strictly serving the College's missions. Because of this possibility, **CaTS** may limit network usage of residential systems. This may be implemented through bandwidth caps, restriction or blocking of services, or other means.

## **6.6 Security**

**Users** are responsible for the security and integrity of their own systems. If a system has been "hacked" or otherwise compromised, **CaTS** shall disconnect it from the network to prevent it from interfering with the proper operation of the network. Reconnection shall only occur after a thorough test of the system has been done by **CaTS** to verify that the any problem has been corrected.

### **6.6.1 Virus Protection**

The residential and wireless networks are shared community resources, which means that a computer "virus," "worm" or similar software can compromise the functioning of the entire network and can infect other computers on the network. Consequently, all computers attached to the residential or wireless networks are required to have an approved "virus protection" program installed and running, and currently updated to include the most recent virus protection offered. Additionally, **Users'** computers connected to the residential or wireless networks must have installed all the operating system "patches" provided by the operating system's software company to fix potential security risks in the operating system.

## **6.7 Abuse**

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

## **6.8 Common Problems: Music files and Software Piracy (warez)**

The distribution of copyright protected materials is illegal and is in direct violation of this **Policy**. Distribution of copyright protected software is similarly prohibited unless the copyright specifically allows redistribution, such as software covered under a "freeware" type license, such as the GNU general public license, or by express permission of the copyright holder.

## **7.0 COMPUTER LABORATORIES**

The Computer Laboratories maintained by Saint Mary's, including those at Extended Education campuses and inside residence halls, are resources installed by the College to promote scholarship and learning for all students. Accidental or intentional disruption of Computer Laboratories will deprive others of access to these important **Computing Resources**. Any Person using Computer Laboratories must comply with all other portions of the College's this **Policy**.

Additionally, the following specific policies apply:

### **7.1 Keys**

Keys to computer labs are issued for use only by the person to whom they are issued.

Keys to computer labs are not to be loaned to anyone. The physical security of computer labs is not to be compromised in any way, including, but not limited to, leaving labs unlocked when not in use, or propping doors open.

## **7.2 Lab Supervision**

Computer laboratories shall not be accessible unless an **CaTS** authorized lab supervisor (i.e., Student Lab Monitor or Instructor with lab access) is on duty in the laboratory. **Users** of the computer labs 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.

## **7.3 Software and Systems**

**Users** are responsible for leaving computers and workspace in laboratories clean and ready for the next **User**. This requires that **User** closes all open applications, logs out of any attached servers, and removes personal items (including diskettes 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.

## **8.0 PROHIBITED ACTIVITIES**

**Users** are subject to all laws and Saint Mary's rules and 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 will result in disciplinary action, loss of computing privileges, and/or legal action.

### **8.1 Abuse of Resources**

**Users** who knowingly and without prior authorization disclose confidential matters will be subject to appropriate discipline by the College, as will those who intercept or enter other College or **User Accounts**, communications, whether or not these relate to confidential matters, will also be subject to discipline, unless 1) the disclosure has also been specifically authorized as provided below, 2) the information was intended to reach the individual receiving the correspondence, 3) the disclosure is necessary to correct improper message routing or to forward miss-routed communications to their intended recipients, 4) the disclosure is to the recipient's supervisor, or other appropriate authority, and the correspondence reached the recipient because of machine or sender routing error, or 5) the disclosure is to the recipients supervisor, and the correspondence seems to contain evidence of improper use of **Computing Resources**, of conduct violating College rule or **Policy**, or of illegal activity.

### **8.2 Examples**

Examples of misuse and prohibited conduct include, but are not limited to, the activities in the following list. It is against Saint Mary's **Policy** to engage in any of these actions:

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**, IP address, computer name or port that you are not authorized/assigned to use.
3. Sharing a password for your **Account**.
4. Deliberately or inadvertently wasting **Computing Resources**.
5. Using **Computing Resources** to harass others, or to create, store, or transmit libelous or obscene materials.
6. Sending chain and junk mail, disseminating mass mail without permission, and creating/distributing mail "bombs."
7. Using **Saint Mary's Computing Resources** to gain unauthorized access to any computer systems. This includes the use of programs such as WinNuke, any sniffer or network monitoring software, Crack or any other software that is used to assist in the compromising of a computer system or **User Account**.
8. Knowingly performing an act that will interfere with the normal operation of third party computers, terminals, peripherals, networks, or any **Saint Mary's Computing Resources**.
9. 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.
10. Using applications that inhibit or interfere with the use of the network by others.
11. Attempting to circumvent data protection schemes or uncover security loopholes.
12. Violating terms of applicable software licensing agreements or copyright laws.
13. Masking the identity of an **Account** or machine, or using a false identity.
14. Posting on electronic bulletin boards materials that violate existing laws, Saint Mary's codes of conduct, or any other Saint Mary's **Policy** applicable to the **User**.
15. 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.
16. Using **Computing Resources** for personal or political gain, including running a business for profit or non-profit purposes, promoting and selling products and services, commercial advertising, commercial businesses not authorized by Saint Mary's, etc.
17. Using **Computing Resources** for political campaigning.
18. Student **Users** may not provide services or **Accounts** from student **User** computers to anyone. (e.g. - web servers, FTP servers, software such as Napster

(running in file sharing mode) that functionally turns a personal computer into a server, etc.)

19. Registering a Saint Mary's IP address with any other domain name (i.e., www.username.com).
20. Capturing passwords or data on the network or Internet not meant for you.
21. Providing a pass-through site to other campus hosts.
22. Modifying or extending Saint Mary's network services and wiring beyond the area of its intended use. This applies to all network wiring, hardware and in-room jacks.
23. To minimize destructive hacking, do not provide information about the networks to News-feeds, Anonymous FTP site, BBSs, etc.
24. Posting private personal information without permission, including but not limited to grades, medical records, or any other information that is protected by law or by Saint Mary's policies.
25. Web pages may not be established on Saint Mary's servers on behalf of non-Saint Mary's organizations, firms, or individuals.

## **9.0 ENFORCEMENT**

### **9.1 Revocation of Privilege and Disciplinary Action**

Saint Mary's reserves the right to limit or deny access to its **Computing Resources** when any Saint Mary's policies 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**. Saint Mary's College will investigate violations of this **Policy** in the same manner as it investigates violations of other Saint Mary's policies or other disciplinary matters. The particular investigative and disciplinary processes that shall be used will depend upon the status of the **User** (e.g., student, faculty, staff, or other). A reference to the full description of the applicable process can be found in the appropriate handbook, employment manual, or employment information packet. **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), may lose the privilege to use **Saint Mary's Computing Resources** for violating this **Policy**.

#### **9.1.1 Minor Violations**

In the case of minor violations, **CaTS** will attempt to contact the **User** by E-mail, telephone, or in person to explain the violation and to attempt a simple resolution of the issue. Should **CaTS** be unable to resolve cooperatively such issues, **CaTS** may take further action as may be necessary to mitigate any potential impairment of other **User's** ability to use **Saint Mary's Computing Resources**, including the temporary removal of **User's** electronic information from **Saint Mary's Computing Resources**.

### **9.1.2 Major Violations**

In the case of major violations, including but not limited to possible violations of law, in addition to invoking any applicable disciplinary process, **CaTS** will immediately attempt to mitigate any actual or potential impairment of other **User's** ability to use **Saint Mary's Computing Resources**, and to mitigate any actual or potential damages that may occur as a result of the violation of federal, state, or local law. Mitigation efforts may include, but are not limited to, suspension of a **User's** access to **Saint Mary's Computing Resources** and the removal of a **User's** web page(s) or other electronic information or data stored on **Saint Mary's Computing Resources**. Prior notice of the suspension or take down is not necessary. **CaTS** will notify the **User** of the violation and of the mitigation action as soon as is practicable under the circumstances.

### **9.2 Discovery of Policy Violations Through Routine Maintenance**

**CaTS** staff occasionally, and randomly, examine the routing information of communications and monitor transactions and traffic across **Computing Resources**, to evaluate, among other issues, volume of traffic and the general use of system resources. Saint Mary's periodically may view the content of material transported across its networks or posted on **Computing Resources** as part of its effort to maintain quality service and reliable delivery of electronic information. **CaTS** has the authority to immediately exclude a **User** from any **Computing Resource** where **CaTS** has a reason to believe that a **User** presently poses or may pose harm to the system or its information and/or data, or where **CaTS** discovers, inadvertently through its routine maintenance activities, possible violations of law or policy.

### **9.3 Reporting**

If a **User** suspects that a particular behavior is in violation of this **Policy**, he or she should contact **CaTS**. Saint Mary's does not expressly monitor the content of **User** web pages and other electronic information, including but not limited to E-mail, for the purpose of enforcement of this **Policy**. However, Saint Mary's will take appropriate action should it become aware of any suspected policy violations (See section [9.2](#) above).

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 shall assist and encourage full enforcement of such laws by the appropriate public entity.

### **9.4 Violations of Law**

In addition to Saint Mary's disciplinary procedures, 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 **Computing Resources**. Blatant or repeated violations of law and/or this Policy, will result in CaTS immediately removing a User's web page or other information from Saint Mary's Computing Resources and the User shall be referred to the appropriate party for disciplinary action.

In the case of copyright infringement, Saint Mary's is bound by certain legal procedures designed to mitigate any damage that may be perpetuated by continuing acts of copyright

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

Policy last revised 05-04-07