SAINT MARY'S COLLEGE OF CALIFORNIA POLICY GOVERNING THE ATTACHMENT AND USE OF PERSONALLY-OWNED COMPUTING EQUIPMENT ON THE SAINT MARY'S NETWORK

Revision Approved May 2016

1.0 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:

2.0 Responsibility

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

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.

3.0 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.

4.0 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.

5.0 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.

6.0 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.

7.0 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.

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.

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).

8.0 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.

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)

Related IT Policies
Saint Mary's College of California Technology Use Policy
Saint Mary's College of California General Policies Governing the Use of Information Technology
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.