NETWORK ACCEPTABLE USE POLICY

College of Saint Mary's (CSM) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CSM's established culture of openness, trust and integrity. CSM is committed to protecting our community from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail or messaging, WWW browsing, are the property of College of Saint Mary.

Effective security is a team effort involving the participation and support of every CSM student and employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment owned by CSM and by students that participate in the College of Saint Mary's data networks.
These rules are in place to protect the students, faculty and staff as well as CSM. Inappropriate use exposes CSM to risks including virus attacks, compromise of network systems and services, and legal issues. This policy applies to students and employees wishing to participate in network related activities on the data networks at College of Saint Mary including all personnel affiliated with third parties.

While CSM 's network administration desires to provide a reasonable level of privacy, users should be aware that administration cannot guarantee the confidentiality of information stored on any network device connected to CSM's network. Students are responsible for exercising good judgment regarding the reasonableness of personal use.

For security and network maintenance purposes, authorized individuals within CSM may monitor equipment, systems and network traffic at any time. College of Saint Mary reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The following activities are, in general, prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. Students may be exempted from these restrictions for legitimate academic purposes as long as the environment is physically or logically isolated from all other routable networks (e.g., a Business Information Systems classes may have a need to port scan a host on the student network).

Under no circumstances is a student or employee of College of Saint Mary authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CSM owned resources.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the student.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CSM or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and friends.

6. Using the CSM network to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access.

For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

8. Port scanning or security scanning is expressly prohibited unless prior notification to Information Services is made.

9. Executing any form of network monitoring which will intercept data not intended for the student's host.

10. Circumventing user authentication or security of any host, network or account.

11. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

13. Providing unauthorized private information about, or lists of, those affiliated with CSM (current or past students, employees, donors, etc.) to parties outside College of Saint Mary including distribution groups or other information specifically intended for the exclusive use of CSM.

14. Disclosing information and/or opinions posted to private forums, discussion boards, Email or classroom discussions without prior expressed consent.

15. All users of network resources are required to logon to the workstations using the credentials supplied at the time of the account’s creation. Any anonymous logons must be limited to guest privileges.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Unauthorized use, or forging, of email header information.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Any individual found to have violated this policy may be subject to disciplinary action, up to and including revocation of network rights or termination.

Term Definition:

Spam – Unauthorized and/or unsolicited electronic mass mailings.