Acceptable Use Policies for Information Technology at the University of Mary

Purpose

To state a consistent framework for the use of University of Mary information technology resources (IT) that allows academic freedom and reasonable access to resources while protecting the resources and its users from misuse of the system.

Statement of the Policy

Access to the University of Mary computing and network resources is a privilege granted by the university to authorized users. This privilege may be suspended with or without notice when continued use of network resources interfere with the work of others, place the university or others at risk, or violate federal, state or local laws or university policy.

The University of Mary's IT resources are intended for the following purposes:

1. research associated with the university curriculum,
2. coursework activities associated with the university curriculum,
3. job responsibilities within the scope of employment at the university,
4. other activities specifically approved by the university information technology department.

The use of university IT is a privilege, not a right. All use of university IT must comply with the Christian, Catholic and Benedictine mission of the University of Mary. All policies of the university apply to the use of its IT regardless of whether the user is associated with the university and regardless of whether the use occurs on campus or remotely.

Authorized users are current faculty, staff and students of the University of Mary and other individuals or organizations specifically authorized by the university.

Agreement

Users of University of Mary IT resources agree to abide by and be bound by the terms of this policy and all policies of the University of Mary.

Users agree that at all times the university has the right to monitor any and all aspects of its IT system, including electronic mail and individual login sessions, to determine if a user is acting in violation of the law or policies of the university.

Standards

1. Users must comply with all applicable law and all university policies. Examples include the laws of defamation, privacy, copyright, trademark, obscenity, child pornography, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the University of Mary's Student Conduct System.

2. Users must comply with all applicable contracts and licenses and shall use software only in accordance with applicable license agreements. All software must be lawfully purchased or acquired.

3. Users may upload or download material through the university's Internet connection subject to full compliance with copyright laws. Users are responsible for recognizing and honoring the intellectual property rights of others. Unauthorized copies of copyrighted material shall not be created, distributed, or knowingly used. Users assume all risk in determining whether material is copyrighted or public domain.

   No use of P2P file sharing applications shall be allowed on any University of Mary computers or networked facilities including university resident hall RESNET without prior approval for academic and other university business. Request for permission may be submitted through a dean or department head, these authorities will then submit a formal written request to the director of IT for approval.

4. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university. Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

5. All users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Users are prohibited from looking at, copying, altering, or destroying another individual's electronic information without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so unless the information has been placed in a public area such as a web site.

6. Users must realize the limits of the university's IT resources and restrict use so as not to consume an unreasonable amount of those resources or interfere unreasonably with the activity of other users. The university may require

users of those resources to limit or refrain from specific uses in accordance with this principle.

Peer-to-peer (P2P) file sharing has been identified as major contributor to this interference and has been identified by the Higher Education Opportunity Act for regulation on college campuses.

7. Only upon written permission from a vice-president of the university and approval by the director of information technology may IT resources be used in connection with compensated outside work or for private business purposes unrelated to the university. Users must otherwise refrain from using university IT resources for personal commercial purposes or for personal financial or other gain. Personal use of university IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

8. Harmful activities are prohibited. Users shall not undermine, hinder, damage, or disrupt the hardware, software, or security of university IT resources. Examples include, but are not limited to, IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

   Expressly prohibited activities include installing any software on the university server and enabling a user to run any programs on the U-Mary server.

9. The University of Mary reserves the right to review and modify material to be made accessible to the public.

Enforcement

Users who violate this policy may be denied access to university IT resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will normally be handled through the university IT department. In its discretion, the IT department may forward violations to appropriate university officials for commencement of disciplinary procedures applicable to the relevant user. The university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other IT resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies. Users who violate this policy are subject to the full range of sanctions, including the loss of IT or network access privileges, disciplinary action, dismissal from the institution,

and legal action. Use that is judged excessive, wasteful, or unauthorized may result in denial of access to IT and networking resources and may subject the user to appropriate disciplinary and/or legal procedures. Any offense which violates local, state, or federal laws may result in the immediate loss of all IT and networking resource privileges and will be referred to appropriate college or university offices and/or law enforcement authorities.

Security and Privacy

The university seeks to protect computer-based information from accidental or intentional unauthorized modification, misuse, destruction, disruption, or disclosure. The University cannot guarantee security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly. In order to make every reasonable effort to protect its IT resources, the university reserves the right to monitor them, as further set forth below.

The university respects the privacy of its users, including their electronic mail. However, the use of university IT resources is not completely private. The normal operation and maintenance of the university's IT resources require backup, caching, logging of activity, monitoring of general usage patterns, scanning of systems and ports and other activities necessary for the rendition of service.

At all times the university has the right to monitor any and all aspects of the system, including electronic mail and individual login sessions, to determine if a user is acting in violation of the law or policies of the university.

Specifically, the university may monitor the activity and accounts of individual users of university IT resources, including electronic mail, individual login sessions and communications, without notice, when (a) the user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of the university or other IT resources or to protect the university from liability; (c) there is reasonable cause to believe that the user has violated, or is violating law or policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; (e) to monitor quality in online academic programs; or (f) it is otherwise required or permitted by law. Any individual monitoring, other than that specified in "(a)", required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the director of the university’s information technology department.

The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual

communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

Approved
November 2009 by the Executive Committee of the University of Mary Board of Trustees