

# The University of Mary Hardin-Baylor

Date: December 2008

## SUBJECT: ACCEPTABLE USE POLICY FOR COMPUTING RESOURCES

The purpose of this policy is to establish procedures for the University of Mary Hardin-Baylor regarding the use of all University information technology equipment and software, including, but not limited to, computers, printers, scanners, video transmissions, and networking equipment and bandwidth. All information technology activities shall support the Christian mission, vision, and philosophy of the University.

### GENERAL

1. Each person with access to the University's information resources is responsible for their appropriate use and by their use agrees to comply with all applicable University policies and procedures and with applicable local, state and federal laws and regulations.
2. This policy defines the boundaries of "acceptable use" of limited University information resources, including computers, networks, information mail services and information sources, as detailed below. It includes by reference a self-contained compilation of specific rules that can be modified as the information environment evolves.
3. The policy is based on the principle that the information environment is provided to support University business and its mission. Other uses are secondary. Uses that threaten the integrity of the system; the function of non-University equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or that are otherwise illegal are forbidden.
4. Users of information systems are required to review and understand the contents of this policy.

### STANDARDS FOR ACCEPTABLE USE

1. The University supports information resources including, but not limited to, the following: computer data facilities and services; computers; networks and the networking infrastructure; email; information and data storage; and video and voice services. These resources are available to faculty, students, staff, guests, and the general public to support the mission of the University.
2. When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced. The priorities for use of University-wide computing resources are:
  - a. *Highest*: Uses that directly support the educational, research and service mission of the University;

- b. *Medium*: Other uses that indirectly benefit the education, research and service missions of the University, as well as and including reasonable and limited personal communications; and
  - c. *Lowest*: Recreation, including game playing, non-education-related streaming media, and downloading/uploading of music, video, or other files unrelated to course assignments.
3. The general standards for the Acceptable Use of information resources require:
- a. Behavior consistent with the mission of the University and with authorized activities of the University;
  - b. Respect for the principles of open expression and academic freedom;
  - c. Compliance with all applicable local, state, and federal laws, regulations, and University policies;
  - d. Truthfulness and honesty in personal and computer identification;
  - e. Respect for the rights and property of others, including intellectual property rights (See the Professional Writing, Research, and Publication Policy); and
  - f. Behavior consistent with the privacy and integrity of information networks, information data and information, and information infrastructure and systems.

## CONTENT AND MISUSE

1. Communications that include threats of violence, obscenity, pornography and/or harassing communications, are prohibited.
2. The use of University computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable University policies), fundraising or advertising on behalf of non-University organizations, or the reselling of University computer resources to non-University individuals or organizations, and the unauthorized use of the University's name, are prohibited.
3. The following activities and behaviors are prohibited (See also the "Intellectual Property" policy.)
  - a. Misrepresentation (including forgery) of the identity of the sender or source of an information communication;
  - b. Acquiring or attempting to acquire passwords of others;
  - c. Using or attempting to use the computer accounts of others;
  - d. Alteration of the content of a message originating from another person or computer with intent to deceive;
  - e. The unauthorized deletion of another person's news group postings;
  - f. The use of restricted-access University computer resources or information without or beyond one's level of authorization;
  - g. The interception or attempted interception of communications by parties not explicitly intended to receive them;
  - h. Making University computing resources available to individuals not affiliated with UMHB without approval from the President's Council;

- i. Making available any materials, the possession or distribution of which is illegal;
- j. The unauthorized copying or use of licensed computer software;
- k. Unauthorized access, possession, or distribution, of information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records;
- l. Intentionally compromising the privacy or security of information;
- m. Intentionally infringing upon the intellectual property rights of others in computer programs or information (including plagiarism and unauthorized use or reproduction);
- n. Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of information chain mail (propagation of SPAM), and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts (See "Broadcast Email Policy");
- o. Failure to comply with requests from appropriate University officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
- p. Unauthorized distribution of passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;
- q. Altering or attempting to alter files or systems without authorization;
- r. Unauthorized scanning of networks for security vulnerabilities;
- s. Attempting to alter any University computing or networking components (including, but not limited to, servers, routers, and switches) without authorization or beyond one's level of authorization;
- t. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;
- u. Intentionally damaging or destroying the integrity of information;
- v. Intentionally disrupting the use of information networks or information systems;
- w. Intentionally wasting human or information resources; and
- x. Negligence leading to the damage of University information, computing/networking equipment and resources.
- y. Gambling on University-owned computers.
- z. Attempting to delay or defer other users from gaining network access

## ENFORCEMENT AND RECOURSE

1. Except as provided by applicable local, state, and/or federal laws, regulations or other University policies, the content of information communications is not by itself a basis for disciplinary action.
2. The University considers any violation of acceptable use principles or guidelines to be a serious offense, and reserves the right to test and monitor security, including copying, examining and deleting any files or information resident on university computer systems allegedly related to unacceptable use.
3. There is no presumption that non-critical data files will be saved beyond useful life such as email and personal files when a student is no longer enrolled or faculty and staff are no longer employed by the University.
4. Persons responsible for policy violations are subject to action in accordance with student, faculty and staff disciplinary policies and procedures and possible prosecution from local, state and federal authorities.

## LIMITATION ON USERS' RIGHTS AND EXPECTATIONS

1. The issuance of a password or other means of access is to assure appropriate confidentiality of UMHB files and information and does not guarantee privacy for personal or improper use of UMHB equipment or facilities.
2. UMHB provides reasonable security against intrusion and damage to files stored on the central facilities. However, UMHB is not responsible for unauthorized access by other users or for loss due to power failure, fire, floods, etc.

## REPORTING AN ABUSE OR FILING A COMPLAINT

To file a complaint or report a violation of this policy, send an e-mail message to [infotech@umhb.edu](mailto:infotech@umhb.edu) or call InfoTech at 254-295-4658.