NOTRE DAME
OF MARYLAND
UNIVERSITY

ACCEPTABLE USAGE POLICIES

FOR

TECHNOLOGY

TABLE OF CONTENTS

Introduction

Notre Dame of Maryland University (NDMU) is committed to providing access for

Privacy and security:

A. The designated NDMU Network Security Administrator may log and monitor certain service and network activities from workstations. These activities include:
   use of passwords and accounts accessed;
   time and duration of network activity;

E-Mail

A NDMU e-mail account is automatically provided for all university employees. E-mail accounts may be accessed both locally and remotely. Local access is obtained by using the campus-standard Exchange client from a campus-assigned workstation. Remote access may be obtained by using Outlook Web Access from other workstations on campus or from an off-campus workstation connected to the Internet.

NDMU recognizes that e-mail users have a substantial interest in privacy with regard to e-mail messages they send and receive. The following policy describes the degree of privacy e-mail users may reasonably assume. University personnel will not read or make available for anyone else to read the contents of any students, faculty, staff member, or authorized party's e-mail files without the permission of the user, unless there are reasonable grounds to do so. Such grounds might include, but are not limited to, maintaining system integrity (such as tracking viruses), meeting legal obligations (such as subpoenas), and performing certain system management functions (such as routing misaddressed messages.)

Requirements for use:

A. Access to the e-mail system may require approval of the appropriate NDMU supervisory or management authority (e.g., department heads, system administrators, etc.).

B. There are no guarantees about the handling of e-mail received from or sent to addresses outside NDMU. Organizations managing e-mail systems elsewhere may or may not have similar policies to those described herein.

C. The account holder is expected to manage all e-mail delivered to that account by suitably disposing of e-mail

Certain uses of the and distribution lists are inappropriate and may be denied. Examples include messages that:

1. Express political or personal opinions.
2. Discuss non-campus related issues.
3.

Prohibited activities and uses:

A. Unlawful messages

Internet

The University provides access to the resources of the Internet to support the curricular and informational needs of the university's members. The facilities to provide this access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to outline the prohibited use of those resources, to provide guidelines for use of Internet resources and to inform employees of certain risks that can occur which may affect NDMU's data and its technology systems. Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources.

Material can be accessed on the Internet that some may consider objectionable or offensive. In no way does NDMU encourage or endorse accessing such material except for legitimate academic purposes. All users are responsible for acknowledging sources, handling potentially offensive material with discretion, and acquiring information which is consistent with one's objectives as a university employee, student or authorized guest. If there is the reasonable expectation that the accessed information would be considered objectionable by some, then public terminals (those in open offices, labs, the library and other public places) may not be used to display such information and hard copy of such information may not be directed to public printers.

Prohibited activities and uses:

A. Except as outlined above, the display of any kind of sexually explicit image or document on any University system is a violation of the University's Sexual Harassment policy (Policy # 6.15 in the Human Resources Policy Manual). In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using NDMU's network or computing resources.

B. Use of NDMU's Internet facilities and computing resources to knowingly violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of NDMU's resources for illegal activity.

C. Use of NDMU facilities to knowingly download or distribute pirated software or data. The NDMU IT department maintains an inventory of all campus-owned software.

D. Use of any NDMU facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

E. Use of any NDMU facilities to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

F. Subscribing another person to a bulletin board or discussion group.

G. Using or distributing unauthorized software.

The Internet is a loosely organized network encompassing hundreds of thousands of computers throughout the world located in academic, commercial, personal, governmental, and organizational sites. There is no central governing body overseeing the network's operation. Due to the nature of the Internet, one should not assume complete security of any transmissions.

Computer Labs

The Rice Hall and Knott Science Computer Labs are available to currently enrolled students, currently employed faculty and staff, and authorized guests. Rice Hall Computer Labs are used for classroom instruction and open lab time; and Knott Science 106 is used for open lab time for students. Both facilities are open up to 100 hours per weekly during the Fall and Spring semesters. Availability varies for Winterim and Summer semesters.

Requirements for use:

A. Class reservations for Rice Hall Computer Labs must be submitted to Conference Services using the Campus Events Scheduling Systems (http://sps.ndm.edu) and can only be made by a university employee.

B. Software required for instruction must be provided to Instructional Services at least one month prior to the start of the semester. All software requests must be compatible with current campus hardware and software standards. The software must be licensed to the University.

C. Peripherals required for instruction must be tested, procured and installed by Instructional Services at least one month prior to the start of the semester. All peripheral requests must be compatible with current campus hardware and software standards.

D. All software used for classroom instruction or to support a lab activity must be tested by the faculty or staff member prior to its use. Testing includes accessing the software and required data files from a lab computer to ensure proper performance.

Social computing labs and workspaces are available to currently enrolled students, currently employed faculty and staff, and authorized guests. These labs are available for academic and social purposes only.

Prohibited activities and uses:

A. Downloading or installing software, not necessary for classroom instruction, on lab computers. Unlicensed software and unauthorized files will be removed from the lab and multimedia workstations.

B. Changing of system settings in any program or application outside of those settings necessary for classroom instruction.

D. Smoking, lighting a tobacco product, or possession of a lit tobacco product.

E. Playing radios, CD players, MP3 players, etc., without the use of headphones.

Acceptable Usage Policy (AUP)

Learning Management System

To assist NDMU in maintaining compliance with applicable policy, procedures, and law, this policy addresses important considerations in the use of Learning Management Systems at the University.

This policy is intended to cover any LMS for which a separate, approved LMS policy does not exist. All LMS-specific use policies must be consistent with this Learning Management System Use Policy. Additional rules and regulations may be adopted by academic and administrative units to meet specific administrative or academic needs. Such additional requirements must be in compliance with applicable federal and state laws, any contractual agreement with the University and vendors and this policy.

Scope

This policy applies to all faculty, staff, students, and others who use an LMS. For the purposes of this policy, an LMS is defined as:

> software for delivering, tracking, and managing NDMU course instruction that
>
> contains personal student data (e.g., name, ID number, email address), regardless of how these data are populated in the LMS.
>
> The "managing unit" is defined as the university academic representative (Faculty Resource Center – FRC) and/or the administrative representative (Instructional Services) who are vested with the day-to-day operations of the LMS.

This policy does not cover use of any LMS for which a separately approved use policy exists (e.g., the Moodlerooms Use Policy)

Policy

Stewardship and custodianship of data brought into or created within the LMS application will be the responsibility

A. LMS managing unit shall restrict course accounts and individual file uploads to a size that permits archiving.

B. Courses shall be retained on LMS for two academic years.

C. The managing unit does not have responsibility for reviewing course content.

D.

A. The managing unit shall notify users of any planned outages of LMS. Notification of any unplanned outages shall be at the discretion of the managing unit. The level of notice for planned outages will be determined by the estimated do