NOTRE DAME
OF MARYLAND
UNIVERSITY

# ACCEPTABLE USAGE POLICIES

# FOR

# TECHNOLOGY

Rev. 06/20/2016

# TABLE OF CONTENTS

## Introduction

Notre Dame of Maryland University (NDMU) is committed to providing access for its community to local, national, and international sources of information and to provide an atmosphere that encourages access to knowledge and sharing of information. The University assumes that information resources will be used by members of its community with respect to and in accordance with guidelines and regulations established by the University. In accordance with the policies stated in this document, the University works to create an intellectual and reasonably secure environment in which students, faculty, and staff are free to create and to collaborate with colleagues both at NDMU and at other institutions. In addition, this policy is intended to support the goal of NDMU to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of students, faculty, staff and guests.  Reasonable steps will be taken to ensure that the products of their intellectual, creative, and professional efforts will not be violated by misrepresentation, tampering, destruction, and/or theft; however, cannot be guaranteed.

This policy defines the boundaries of acceptable use of NDMU’s technology resources, including computers and peripherals, data, networks, software, Internet, electronic mail services, telephone services, computer labs and hi-tech classrooms.  These Information Technology (IT) resources are to be used for university-related purposes.  This policy applies to all users of university IT resources, whether affiliated with the university or not, to all users of those resources, whether on campus or from remote locations.  All users are responsible for adhering to the University’s Acceptable Use Policy.

Users who violate this policy may be subject to penalties and disciplinary action, including expulsion, dismissal, or revocation of user access.

## General Rules

NDMU's technology resources are the property of NDMU. They are to be used for the advancement of NDMU instruction, academic research, learning, service, community outreach, administrative and business purposes, and for communication among employees and students. Users of University IT resources must comply with federal and state laws, university rules, regulations and policies, and the terms of applicable contracts including software licenses while using IT resources. Examples of applicable laws, rules and policies include but are not limited to the laws of libel, privacy, copyright (www.copyright.gov ), trademark (www.uspto.gov/trademarks/index.jsp ); the Maryland Computer Crimes Act, the Electronic Communications Privacy Act (www.it.ojp.gov/default.aspx?area=privacy&page=1285 ) , the Computer Fraud and Abuse Act, the university's Honor Code (www.ndm.edu/student-life/honor-code ), the university's Policy on the Use of the University Name and Logos, and the university's E-mail Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

Campus technology resources are provided for the use by current employees (faculty and staff), students, and other properly authorized guests.

A. When an employee's affiliation with NDMU ends, NDMU will terminate access to the campus' technology resources and accounts.

B. Access to campus technology resources and accounts will terminate when a student withdraws from the University or 6 months after graduation.

C. Access and technology privileges extended to campus guests will be terminated when their affiliation with the University ends.

D. Requests for extension of privileges may be made through appropriate chairperson, department directors or other administrative personnel.

**Requirements for the use of technology:**

A. Users must comply with all applicable local, state, and Federal laws and regulations, this policy, NDMU's honor code and other applicable policies.

B. Never login under any username other than the one provided to you by NDMU and never use a device logged in as any user other than yourself.

C. Users must be truthful and accurate in personal and computer identification.

D. Users must respect the rights and privacy of others.

E. Users must not compromise the integrity of electronic networks and must refrain from activities that may damage the network, transmitted or stored data.

F. Users must maintain the security of accounts by protecting and regularly changing their account passwords. Individuals responsible for system administration are required to regularly change passwords to protect information and maintain security.

## Prohibited activities and uses:

A. Threats of violence, obscenity, pornography, and harassing communications, and any other unlawful communications. 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. Unauthorized use of University resources for any and all activities not related to University business, including use of NDMU resources for private business or commercial activities, fund raising or advertising on behalf of non-NDMU organizations.

C. Reselling of NDMU computer resources.

D. Unauthorized use of University trademarks, logos and other protected forms of intellectual property, including faculty-produced software for classroom use.

E. Misrepresenting or forging the identity of the sender or the source of an electronic communication.

F. Acquisition, attempts to acquire, and the unauthorized use of passwords of others.

G. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization.

H. Unauthorized modification of or deletion of another person's files or account.

I. Altering the content of a message originating from another person or computer with intent to deceive.

J. Intentionally or recklessly compromising the privacy or security of electronic information.

K. Scanning of networks for security vulnerabilities, account information or unauthorized content.

L. Interference with or disruption of NDMU's computer or network accounts, services, or equipment. The intentional propagation of computer "worms" and "viruses," sending electronic chain mail, denial of service attacks, and inappropriate "broadcasting" of messages to large numbers of individuals or hosts.

M. Wiring, including attempts to create network connections, or any extension or re-transmission of any computer or network services unless approved by an authorized Information System's network administrator.

N. Negligent or intentional conduct leading to disruption of electronic networks or IT.

O. Negligent or intentional conduct leading to the damage of NDMU electronic information, computing/networking equipment (including, but not limited to workstations, bridges, routers, and hubs) and resources.

## 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;
- access to network software;
- volume of data storage and transfers; and
- server space used for e-mail and stored objects.

B. Software and physical limitations, computer viruses and third party intrusions can compromise security of data storage and communications. NDMU takes reasonable precautions to minimize risk. Although nightly backups of server programs and data are performed, NDMU is not obligated to maintain back-ups of any file for extended periods of time. Individual users and departments should develop policies and practices to ensure regular backups of data found on departmental workstations.

C. All NDMU departments should implement policies to ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords restricting access to information should be changed on a regular basis and systems should be developed and implemented to assure password records are regularly updated by appropriate supervisors.

D. Software not installed by the IT department that adversely affects the integrity of the NDMU workstation or network will be subject to removal by the designated Network Security Administrator.

## 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 in the account's mailbox (deleting messages, transferring messages to a personal computer's storage, or saving messages to files in the account's home directory on the campus network). Managing e-mail also requires account holders to suitably control the automatic delivery of messages from such services as mailing lists (i.e. Listserv and Comserve) and newsletters.

D. Electronic storage for mailboxes is limited and IT must ensure that sufficient space is available for the on-going delivery and receipt of new messages.

E. The accumulation of a large volume of e-mail in an account's mailbox may require IT to take management action such as deletion of dated messages. A large volume of unread e-mail being received by an account can cause network, mail performance and storage problems. A reasonable attempt will be made to contact university employees prior to an account being purged due to inactivity.

F. Campus distribution lists are made available for use the Executive Leadership Team (ELT) and their designees. Discretion must be used when utilizing these lists.

- Messages to the **All Faculty, Assoc. Faculty,** and **All Staff** distribution lists are for campus business only. When sending e-mail to All Faculty, Assoc. Faculty, and All Staff, do not include any other distribution lists (campus or personal) or off-campus e-mail addresses in the TO or CC lines.

- Certain uses of the **All Faculty** and **All Staff** 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. Solicit donations to charitable causes not sanctioned as a campus endeavor by Human Resources or Campus Activities.
  4. Serve to market non-NDMU goods and/or services.
  5. Contain potential virus information. (These should be forwarded to the Help Desk at HelpDesk@ndm.edu.)

- When sending e-mail to **student** distribution lists, do not include any other distribution lists (campus or personal) or off-campus e-mail addresses in the TO or CC lines.

- When sending e-mail to students, remember the following account information and sending guidelines.

## Student Requirements for Use

NDMU has over 10,000 student e-mail accounts using the Microsoft Office 365 NDMU student account-for-life program. NDMU e-mail accounts are automatically provided for full and part-time students. These e-mail accounts may be used by students for life. They have no expiration date and are subject to the offer extended to all academic institutions through Microsoft Corporation, Inc. NDMU makes no expressed guarantee as to the length of time Microsoft will extend this offer and relies on the good faith of Microsoft Corporation to support this program into perpetuity, or at such time as Microsoft no longer supports this program.
E-mail accounts may be accessed both locally and remotely. 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.)

Students may:
1. Only access their Notre Dame E-mail accounts through Microsoft 365;
2. Use many different computer or mobile device configurations to access e-mail through the Internet. User experience may vary from device-to-device. If there is a significant reduction in service or performance, then contact the HELP desk for assistance (x5200).

## Guidelines

Students should:
1. Avoid sending large attachments over 10 MB;
2. Avoid using graphics and special fonts. These may be difficult for students to view. Messages should be as simple as possible. They can be attractive and readable without the extensive use of pictures, special fonts and colors

## Prohibited activities and uses:

A. Unlawful messages, including threats of violence, obscenity, pornography, and harassing communications.

B. Use of NDMU e-mail for private business or commercial activities, fund raising or advertising on behalf of non-NDMU organizations.

C. Misrepresenting or forging the identity of the sender or the source of e-mail.

D. Altering the content of an e-mail message originating from another person or computer with intent to deceive.

E. Interference with or disruption of the e-mail accounts and services.  The intentional propagation of computer “worms” and “viruses,” the sending of electronic chain mail, denial of service attacks, and inappropriate "broadcasting" of messages to large numbers of individuals or hosts.

## 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.

**Word of Caution:**

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.

### Instructional Classrooms and Workspaces

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.

## Technology-Enabled Classrooms / 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 Technology-Enabled Classrooms and Labs, requiring a classroom or lab for the entire semester, must be submitted your department chair in preparation the semester.

B. Individual reservations for Technology-Enabled Classrooms and Labs must be made using the Campus Events Scheduling Systems (http://sps.ndm.edu) and can only be made by a university employee.

C. Semester changes to move your class to another classroom, must be submitted to your department chair.

D. 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.

E. 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.

F. 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.

### 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.

## 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

### Data Governance

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

### LMS Use, Operations and Security

A. All users of LMS must authenticate with unique user credentials.

B. All users of LMS must adhere to the Acceptable Use Policy and the University’s Honor Code.

C. All users of LMS must not use the system for purposes other than NDMU-affiliated activities.

D. NDMU is not responsible for the accuracy, integrity, and/or legality of the content uploaded to LMS.

### User management and access

A. All users of LMS must access the system through a designated account.

B. IT has the authority to shall disable access or remove users for inappropriate behavior, per the University's Acceptable Use policy and other policies that define appropriate conduct for University employees and students. IT also has the authority to shall disable access or remove users at the request of Academic Affairs and/or Human Resources.

## Access to LMS

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. The managing unit shall remove illegal content or content that is in violation of University policies or contractual agreements from a course account if requested by the instructor of record or other appropriate University official.

E. Colleague is the sole repository of official course grades and rosters. While roster and gradebook information in LMS is confidential, LMS is not the official record of course grades and rosters.

## Organization management and access

A. University employees, academic and administrative units, and student organizations may request organization accounts.

B. Organization accounts must be related to official University business or activities.

C. Organization accounts for students must be approved by the Student Life.

D. The total number of organization accounts shall be restricted to allow for the adequate functioning of the system.

E. The managing unit shall remove illegal content or content that is in violation of University policies or contractual agreements from an organizational account by request of the organization leader or other appropriate University official.

## Content management and access

A. Delivery and access to copyright materials in LMS must adhere to copyright guidelines set forth by the Library of Congress (www.copyright.gov).

B. The University is not responsible for content linked from LMS to external web sites.

## Support and Training

A. The managing unit shall designate technical support to assist with LMS support and training for faculty and students.

B. The managing unit(s) shall support leaders of organization accounts.

## System Maintenance, Outages, Upgrades

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 downtime of the system.

B. Faculty should consider planned outages when scheduling assignments and tests, and unplanned outages when such outages interfere with the timely completion of student coursework.

C. The managing unit shall be responsible for deploying new features to LMS.

## Enforcement

A. The managing unit will enforce and establish standards, procedures, and protocols in support of the policy.

B. The managing unit will enforce the AUP and establish standards, procedures, and protocols in support of the policy. Violations of this AUP may result in suspension or termination of access to computing accounts, the network and networked resources, and/or other University-owned technology devices.  Violations of law may also be referred for criminal or civil prosecution.

C. The managing unit has the authority to remove or disable access to LMS without notification in the event of law violation or systems compromise involving restricted data as defined by the Data Classification Policy.