

## Notre Dame de Namur University

### Acceptable Use Policy for Information Technology

- A. **PURPOSE** - NDNU owns and operates a variety of computing systems for University-related use by NDNU students, faculty and staff in support of the educational and administrative programs and processes of the University. These systems are to be used only for these University programs and processes. Commercial and other non-University uses are specifically excluded. All students, faculty and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical and lawful manner. This document defines acceptable use of these University computing systems. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as prosecution under Federal and State penal laws.
- B. **RIGHTS** - NDNU reserves all rights, including termination of service without notice, to the computing resources that it owns, operates or permits to operate on its systems or servers. This policy and related procedures shall not be construed as a waiver of any rights of NDNU. Users of University hardware, software, servers and email systems do not have a right of privacy to any information on these systems, regardless of any investment of time or resources by them. The University retains the right to access all such systems, without or with notice, for any reason related to University functions.
- C. **AUDIENCE and AGREEMENT** - All users of NDNU computing systems must comply with this policy and related procedures, as well as any additional guidelines established by the administrators of each specific computing system. Such guidelines will be reviewed by the chair/ supervisor/program director, and, if necessary, by the Provost and/or Vice President for Administration. By using any of these systems, users agree that they will comply with this policy.
- D. **PRIVILEGES** - Access and privileges on NDNU computing systems are assigned and managed by the administrators of specific computing systems. Eligible individuals may become authorized users of a specific system and be granted appropriate access and privileges by following the approval steps prescribed for that specific system. Users may not under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without explicit permission from the specific systems administrator. The authorized user is responsible for proper use of the specific system, including reasonable password protection.

**E. RESPONSIBILITIES** - Users of NDNU Computing Systems:

1. Shall be responsible for maintaining an environment which is conducive to the educational and administrative functions of the University and in which resources are shared equitably between and among users.
2. Shall not use the systems for purely personal uses, to access pornography, to access other materials which are unlawful to access or possess, to access materials for uses unrelated to legitimate University activity or for commercial purposes. Commercial purposes are those for which, in whole or in part, the user seeks financial or similar gain for individuals or entities other than the University.
3. Shall not harass or make defamatory or derogatory remarks using the NDNU voice or data networks. The University's Policy Against Sexual and Other Unlawful Harassment applies fully to use of all University systems. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions.
4. Shall not engage in activity that may compromise the system integrity or security of any on or off-campus system. This includes any type of unauthorized access or hacking.
5. Shall not engage in unauthorized monitoring of individual User activity, information and communications.
6. Shall ensure the security of restricted, confidential, proprietary, licensed, copyrighted or sensitive information entrusted to their care or that may come into their possession. Security includes, as appropriate, protection from unauthorized disclosure, modification, copying, destruction or prolonged unavailability.
7. Shall understand that NDNU computing systems provide access to outside networks both public and private which furnish electronic mail, information services, bulletin boards, conferences, etc. NDNU does not assume responsibility for the contents of any of these outside networks. Users agree to comply with the acceptable use guidelines for whichever outside networks or services they may access through NDNU systems. Further, the user agrees to follow proper etiquette on outside networks.
8. Shall agree never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which s/he is authorized, or any attempt to deprive other authorized users of resources or access to any NDNU computer system shall be regarded as malicious and may be treated as an illegal act.
9. Shall not copy computer software, or other materials protected by copyright or trademark, from, into, or by NDNU computing facilities, except as permitted by law or by the contract

with the owner of the copyright or trademark. This means that such computer and microcomputer software or protected documents may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

10. Shall not use a knowledge of passwords or of loopholes in computer security systems to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given. Other individuals shall not use any account assigned to an individual without explicit permission from the systems administrator. Users are not under any circumstances to confer these privileges to other individuals.

## **F. VIOLATIONS and ENFORCEMENT**

1. The Director of OIT shall have the primary responsibility for promulgation and enforcement of this policy, except this enforcement through discipline of the faculty, staff or student shall follow the respective University policies and procedures governing such discipline. It shall be the Director's responsibility to make every user of NDNU computing systems aware of this Policy and to make initial determinations of violations of the policy when possible violations are brought to his or her attention.
2. Immediately upon the Director of OIT finding evidence which s/he believes indicates that an individual is in violation of this policy, the Director will notify appropriate campus officials of the possible violation. If the individual is a student, the Director will notify the Associate Provost for Student Affairs and Dean of Students. If the individual is an employee, the Director will notify employee's supervisor, the Provost or the Vice President in whose area the employee works, and the Director of Human Resources. Such notices shall be in writing, shall state the nature of the potential violation, and shall describe the evidence that suggests a violation occurred. The appropriate campus officials will determine appropriate action, which may include the individual losing his or her privileges to use NDNU computing systems, either immediately or after informal or formal processes.
3. Privileges removed as a result of violations of this policy will be reinstated only with the approval of the relevant Vice President or the Provost. Such reinstatement may be after informal or formal processes.