ATENEO DE DAVAO UNIVERSITY
E. Jacinto St., 8016 Davao City, Philippines
Tel No. +63 (82) 221.2411
In Consortium with Ateneo de Zamboanga University and Xavier University

University Information Technology Office
Locals: 8206, 8247; Fax +63 (82) 222.3090
E-Mail: uito@addu.edu.ph
Intranet website: http://uito.addu.edu.ph

Policy on Acceptable Use of Electronic Resources

1. Overview
   1.1. This policy on acceptable use of electronic resources defines the boundaries with respect to the acceptable use of electronic resources.
   1.2. Electronic resources include, but are not limited to computer facilities and services, computers, networks, electronic mail, electronic information and data, and video and voice services.
   1.3. Ateneo de Davao University makes these electronic resources available to faculty, students, staff and registered guests to support the educational, research and service missions of the University.
   1.4. All members and registered guests of the University community are responsible for the integrity of these resources. Respect for the integrity of these resources means respecting the integrity of the physical facilities and controls of the University and University-leased systems and respect for all pertinent licenses and contractual agreements.
   1.5. When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced.
      1.5.1. Under certain unusual circumstances, a system administrator is authorized to access a user's computer files to keep the performance of a University IT system from degrading. The said action must be logged by the system administrator.
      1.5.2. Authorized faculty and staff may set and alter priorities for exclusively local computing/networking resources.
      1.5.3. The priorities for use of University-wide computing resources are:
         1.5.3.1. Highest: uses that *directly* support the educational, research and service missions of the University
         1.5.3.2. Medium: uses that *indirectly* benefit the education, research and service missions of the University
         1.5.3.3. Lowest: reasonable and limited personal communications
         1.5.3.4. Forbidden: all activities in violation of the General Code of Conduct and the Faculty Handbook (and whatever counterpart documents these may be) or activities prohibited in the Specific Rules interpreting this policy
      1.5.4. The University may enforce these priorities by restricting or limiting usages of lower priority in circumstances where their demand and/or limitations of capacity impact or threaten to impact usages of higher priority.
   1.6. The responsibilities of each user are the following:
      1.6.1. Each person with access to the University's computing resources is responsible for their appropriate use, and by their use agrees to comply with all applicable University

policies and regulations as well as national and local government regulations. Acceptable use policies extend to the use of affiliated networks and systems.

1.6.2. Each user is expected to use only those computer services, networks and accounts which the University has authorized for his/her access, and to use them only for the purposes for which they were issued.

1.6.3. Each user is responsible for all use of all the accounts issued for his/her use. Consequently, each user is responsible for protecting his/her passwords. Users are not allowed to reveal computer account passwords.

1.6.4. Each user's electronic mail is to be treated as the use of postal services. Email messages are to be opened and read by the user to whom they are addressed.

1.6.5. A user is not allowed to attempt to gain control of any files or computers without the prior consent of the "owner" of those files or computers.

1.6.5.1. The system administrator does not give consent for users to gain control of any network servers, routers or switches.

1.6.5.2. The system administrator does not give consent for users to 'look around' the file systems on any server.

1.6.6. Each user is responsible for reporting unauthorized use of his/her accounts to the University Information Technology Office (UITO).

1.7. Data owners – whether departments, units, faculty, students, guests or staff – may allow individuals other than University faculty, staff and students access to information for which they are responsible, as long as such access does not violate any license or contractual agreement, University policy, or any national or local law or ordinance.

2. General Standards for the Acceptable Use of Computer Resources

2.1. Failure to uphold the following General Standards constitutes a violation and may be subject to disciplinary action.

2.2. The General Standards require:

2.2.1. Responsible behavior with respect to the electronic information environment at all times;

2.2.2. Behavior consistent with the mission of the University and with authorized activities of the University or members of the University community;

2.2.3. Respect for the principles of open expression;

2.2.4. Compliance with all applicable laws, regulations and University policies;

2.2.5. Truthfulness and honesty in personal and computer identification;

2.2.6. Respect for the rights and property of others, including intellectual property rights;

2.2.7. Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and

2.2.8. Respect for the value and intended use of human and electronic resources.

2.3. Enforcement and penalties for violations

2.3.1. Any person who violates any provision of this policy, of the Specific Rules interpreting this policy, of other relevant University policies, or of applicable local or national laws may face sanctions up to and including termination or expulsion. Depending on the nature and severity of the offense, violations can be subject to disciplinary action through the Student Disciplinary System or procedures applicable to faculty and staff.

2.3.1.1. It may, at times, be necessary for authorized systems administrators to suspend someone's access to University computing resources immediately for violations of this policy, pending interim resolution of the situation (for

example by securing a possibly compromised account and/or making the owner of an account aware in person, that an activity constitutes a violation).

2.3.1.2. In the case of egregious and continuing violations, suspension of access may be extended until final resolution by the appropriate disciplinary body.

2.3.1.3. System owners, administrators or managers may be required to investigate violations of this policy and to ensure compliance.

3. Specific Rules Interpreting the Policy on Acceptable Use of Electronic Resources

3.1. Overview: The following specific rules apply to all uses of University computing resources. These rules are not an exhaustive list of proscribed behaviors, but are intended to implement and illustrate the General Standards for the Acceptable Use of Computer Resources, other relevant University policies, and applicable laws and regulations. Additional specific rules may be promulgated for the acceptable use of individual computer systems or networks by individual departments or system administrators.

3.2. Specific Rules

3.2.1. Content of communications:

3.2.1.1. Except as provided by University policies or regulations and local or national laws, the content of electronic communications is not, by itself, a basis for disciplinary action.

3.2.1.2. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law) are prohibited.

3.2.1.3. 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.

3.2.2. Identification of users:

3.2.2.1. Competent University authority may direct an authorized system administrator to attempt to identify the originator of anonymous/pseudonymous messages which are in violation of University rules and regulations, or of local and national law, and may refer such matters to appropriate disciplinary bodies to prevent further distribution of messages from the same source.

3.2.2.2. The following activities or behaviors are prohibited:

3.2.2.2.1. Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication;

3.2.2.2.2. Acquiring or attempting to acquire passwords of others;

3.2.2.2.3. Using or attempting to use the computer accounts of others;

3.2.2.2.4. Alteration of the content of a message originating from another person or computer with intent to deceive; and

3.2.2.2.5. The unauthorized deletion of another person's news group postings

3.2.3. Access to computer resources

3.2.3.1. The following activities or behaviors are prohibited

3.2.3.1.1. The use of restricted-access University computer resources or electronic information without or beyond one's level of authorization;

3.2.3.1.2. The interception or attempted interception of communications by parties not explicitly intended to receive them without approval of an authorized University official

3.2.3.1.3. Making University computing resources available to individuals not affiliated with the University without approval of an authorized University official;

3.2.3.1.4. Making available any materials the possession or distribution of which is illegal;

3.2.3.1.5. The unauthorized copying or use of licensed computer software;

3.2.3.1.6. Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records;

3.2.3.1.7. Intentionally compromising the privacy or security of electronic information;

3.2.3.1.8. Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use of reproduction)

3.2.4. Operational Integrity

3.2.4.1. The following activities and behaviors are prohibited:

3.2.4.1.1. 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 electronic chain mail, and the inappropriate sending of "broadcast messages" to large numbers of individuals or hosts.

3.2.4.1.2. 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;

3.2.4.1.3. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;

3.2.4.1.4. Altering or attempting to alter files or systems without authorization;

3.2.4.1.5. Unauthorized scanning of networks for security vulnerabilities;

3.2.4.1.6. Attempting to alter any University computing or networking components (including, but not limited to, bridges, routers and hubs) without authorization or beyond one's level of authorization;

3.2.4.1.7. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;

3.2.4.1.8. Intentionally damaging or destroying the integrity of electronic information;

3.2.4.1.9. Intentionally disrupting the electronic networks or information systems;

3.2.4.1.10. Intentionally wasting human or electronic resources;

3.2.4.1.11. Negligence leading to the damage of University electronic information, computing/networking equipment and resources