

NATIONAL-LOUIS UNIVERSITY

HUMAN RESOURCES POLICY AND PROCEDURE

POLICY TITLE:	Acceptable Use of Information Technology
EFFECTIVE DATE:	January 2005
SCOPE:	All Prospective Students, Students, Staff, Faculty, Board Members, Alumni and Administrators

PURPOSE

The Acceptable Use Policy outlines user responsibilities and provides a framework for accountability for appropriate use of the University Information Technology and Services.

National-Louis University provides resources to the University community (which includes all prospective students, students, staff, faculty, board members, alumni, and administrators) through its Information Technology and Services.

Use of Information Technology and Services must be consistent with the mission, goals and objectives of the University. University community members are responsible for their activities and accountable for their individual conduct while using University Information Technology and Services.

The contents of the University Information Technology and Services are owned by the University, with the exception of any content specifically covered by University intellectual property agreements or contractual obligations.

POLICY

National-Louis University community members:

1. Are responsible for abiding by all laws applicable to their use of University Information Technology and Services. This includes but is not limited to those laws dealing with copyrights, trademarks, patents, privacy and intellectual property laws.
2. May use University Information Technology and Services for educational, instructional, service, research, administrative and other purposes consistent with their roles in the University community. Incidental personal use of University Information Technology and Services is allowed if:
 - a. It does not interfere with the operations of and University Information Technology and Services, as determined by any IT professional staff member and;
 - b. It does not interfere with the job performance of staff or faculty, as determined by the supervisor.

3. May not use University Information Technology and Services for commercial activity, other than University sponsored and authorized activities.
4. May not use University Information Technology and Services for political, religious or other advocacy purposes unless related to the academic expertise and responsibilities of a faculty member.
5. Are responsible for respecting the integrity of the University Information Technology and Services including but not limited to:
 - a. Refraining from activities to gain unauthorized access to or use of University Information Technology and Services which are intended to circumvent security measures and;
 - b. Any activities which would interfere with the normal operations of the University Information Technology and Services.
6. Are responsible for conducting themselves in a professional and ethical manner in all communications conducted via University Information Technology and Services.
7. Have the right to due process, consistent with respective policies governing the categories of users, in cases of discipline resulting from violations of the guidelines as outlined in this policy.

PROCEDURE

Guidelines to the National-Louis University Policy on Acceptable Use of University Information Technology and Services

Definitions:

National-Louis University Information Technology and Services refers to all computers and Information Technology and Services owned or operated by the University and include: hardware, software, data, communication networks associated with these systems and services. These systems range from multi-user systems to single-user terminals and personal computers, whether freestanding or connected to networks.

System users are all those individuals with privileges to use University Information Technology and Services; including but not limited to students, faculty, University staff and administrative officers.

Deans and Vice Presidents, with the assistance of System Administrators, will determine who is permitted access to a particular system. System Administrators and other designated system users hold responsibility for the maintenance and security of University Information Technology and Services as a part of their stated responsibilities as academic or non-academic employees. System Administrators report directly to the Collegis/University Technical Director. The Collegis/University Technical Director directly reports to the Collegis/University Executive Director who reports directly to the designee of the University President. The Collegis/University Executive Director holds ultimate responsibility for the maintenance and security of NLU Information Technology and Services.

1. Adherence to Laws Governing Ownership and Copyright Law
 - a. Users must observe intellectual property rights including, in particular, copyright laws as they apply to software and electronic forms of information.
 - b. Users may use only legally obtained, licensed data, or software in compliance with license or other agreements and federal copyright and intellectual property laws.
 - c. Users shall not place copyrighted material (software, images, music, movies, etc.) on any University computer without prior permission from the copyright holder or as granted in a license agreement or other contract defining use.
2. Authorized Use
 - a. Individuals using University Information Technology and Services and must be identified either through the physical location of an office or instructional computer or through an authorized University computer account, as with multiple user systems. System users may not access or use another user's computer account or allow another person to use his or her account.
 - b. System Administrators create accounts and regulate access to University Information Technology and Services by authorized system users. System administration privileges are granted only for official purposes and under the authority of designated academic and administrative officers. Unauthorized usage or assignment of administrative privileges is expressly prohibited.
 - c. Users must not conceal their identity when using University Information Technology and Services, except when anonymous access is explicitly provided (as with anonymous ftp).
 - d. University Information Technology and Services may not be used as a means of unauthorized access to computing accounts or systems inside of or outside of University Information Technology and Services. Other uses of University Information Technology and Services may be permissible including revenue generating activities subject to policies and procedures governing contractual agreements.
3. Privacy
 - a. All access to protected information stored in University record systems will be in strict compliance with the provisions of Federal and State laws. The Family Educational Rights and Privacy Act (FERPA) or "Buckley Amendment" (34 C.F.R. Part 99, as amended by 61 Fed. Reg. 59291 Nov. 21, 1996) provides for protection against unwarranted disclosure of private information contained in "official" University records. FERPA guarantees all postsecondary students the right to consent to disclosures of personally identifiable information contained in student education records, except to the extent that FERPA authorizes disclosure without consent. For additional information, see <http://www.edlaw.net>.
 - b. Computer users must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data files without the consent of the

individual or individuals involved. Administrative users may inspect or repair data files (including e-mail stored on University mail systems) as required as part of their employment, and then only to the extent necessary to maintain the integrity and operations of University Information Technology and Services.

- c. University employees and others may not seek out, examine, use, modify, or disclose, without authorization, personal or confidential information contained in a computer, which they access as part of their job function. Employees must take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties.
 - d. Use of Internet systems to transmit information does not guarantee privacy and confidentiality. Sensitive material transferred over University Information Technology and Services (including e-mail and the World Wide Web) may be at risk of detection by a third party. Users should exercise caution and care when transferring such material in any form.
4. The following uses of University Information Technology and Services are specifically prohibited due to their malicious and destructive nature:
- Use of computer programs to decode passwords or access control information.
 - Attempts to circumvent or subvert system or network security measures.
 - Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to University data.
 - Wasting computing resources or network resources; for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain-letters or unsolicited mass mailings.
 - Using mail or messaging services to harass, libel, intimidate, or distribute misinformation, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or user ID.
 - Users must not access or attempt to access data on any system they are not authorized to use. Users must not make or attempt to make any deliberate, unauthorized changes to data on a University system. Users must not intercept or attempt to intercept data communications not intended for that user's access, for example, by "promiscuous" bus monitoring or wiretapping.
5. Enforcement
- a. Authorized System Administrators may monitor computer activity for the sole purpose of maintaining system performance, security, and integrity. In instances when individuals are suspected of violating policies, the contents of user files may be inspected only upon the approval of the University officer having clear responsibility for the activity of the user.
 - b. At the discretion of the System Administrator(s) responsible for the resource or service in question, in collaboration with the appropriate

administrative authority, information system computer use privileges may be temporarily or permanently revoked, following due process appropriate for the parties involved, pending the outcome of an investigation of misuse, or finding substantiating violations of these guidelines.

6. Due Process

- a. University Information Technology and Services users have the right to due process (consistent with respective policies governing the categories of users) in cases of discipline resulting from violations of the guidelines outlined in this document.
- b. When a System Administrator believes it necessary to preserve the integrity of facilities, user services, or data, he or she may suspend any account, whether or not the account owner (the user) is suspected of any violation. Where practical, 24-hour notice will be given in advance of revocation.
- c. If, in the judgment of the System Administrator, the violation warrants action beyond a System Administrator's authority, he or she will refer the case first to the University administrator or disciplinary body appropriate to the violator's status (e.g., in the case of a faculty member, his/her dean), and, as deemed appropriate, to a law enforcement authority.
- d. A University Information Technology and Services user accused of a violation will be notified of the charge and have an opportunity to respond (consistent with respective policies governing the categories of users) before a final determination of a penalty. If a penalty is imposed, the accused violator may request a review by the designated administrator or body empowered to assure due process and an impartial and timely review of the charges.

NOTE:

National-Louis University supports the EDUCAUSE Code of Software and Intellectual Rights. Users should consider the EDUCAUSE Code as a standard to guide their ethical use of electronic resources and information:

- Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.
- Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.