



Personnel Policies for Lincoln University

The guiding principle for these policies is *The Rules and Regulation of Lincoln University • Chapter I University Governance: Structure and Functions • Chapter VI Administration and Finance • Chapter VIII University Employment • HRSHB 6.1*

Effective August 13, 2009

Technological Resources

Letter from the President

Rules and Regulations

Adjunct Handbook

 Print using your browser's print function.

Faculty Handbook

 Print using your browser's print function.

Staff Handbook

 Print using your browser's print function.

Employees covered by this policy

This policy applies to all Faculty, Staff and Hourly employees at LU and applicants of positions.

Policy

An employee's use of Lincoln University technology resources is subject to federal, state, and local law and university regulations. A comprehensive listing of technological resources can be found on the Lincoln University website.

Users of technological resources must observe intellectual property rights, in particular, the software copyright law. Users must refrain from using university trademarks or logos without prior authorization and from implying, by use of Lincoln University technological resources, that the person speaks for the university.

Except in cases of explicitly authorized external access, such as for incoming electronic mail, anonymous ftp or similar services, or specially authorized external users, Lincoln University computing resources are limited to members of the LU community. Users must not permit or assist any unauthorized person in accessing OIT facilities. Authorization for other external use of the university's computing resources by outside organizations or individuals requires written approval of the president, and will be granted only when that use is determined to further the university's mission.

Another person may not use an account assigned to an individual. Staff is individually responsible for the proper use of their accounts, including proper password protection and appropriate use of computing resources.

Users of university computing resources, including microcomputers, workstations, printers, or other public facilities, must show identification upon request by members of the Lincoln University Department of Public Safety, OIT staff, or any other authorized university official.

All use of university computers and networks must be consistent with all contractual obligations of the university, including limitations defined in software and other licensing agreements.

Users shall observe all applicable policies of external data networks when using such networks, including sites visited via the Internet.

Users must allow OIT personnel access to data files kept on OIT systems for the purpose of systems backups or diagnosing systems problems, including rules violations.

Without specific authorization, all activities conducted through Lincoln University computing resources for personal profit or for the direct financial benefit of any non-Lincoln University organization are prohibited. However, this is not meant to restrict normal communications and exchange of electronic data, consistent with the university's education and research roles that may have an incidental financial or other benefit for an external organization. For example, it is appropriate to discuss products or services with companies doing business with Lincoln University or to contribute to Usenet bulletin boards discussing issues relating to commercial products.

Incidental personal use of university computing resources may be allowed when such use does not interfere with university operations, does not compromise functioning of the university's network, or does not interfere with the user's employment or other obligations to the university.

University computing resources may not be used to threaten or harass any person. A user must cease sending messages or interfering in any way with another user's normal use of computing resources if the aggrieved user makes a reasonable request for such cessation. The university's Sexual Harassment policy is extended to include harassment via computing resources.

Without specific authorization, users of OIT computing or network facilities may not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, reconfiguration of control switches or parameters, or changes in firmware. This rule seeks to protect "data, computing, and communications equipment" owned by OIT, Lincoln University, or any other person or entity. "Specific authorization" refers to permission by the owner or designated administrator of the equipment or data to be destroyed or modified.

Without specific authorization by the owner or designated administrator, users may not remove any university owned or administered equipment or documents from a university facility.

Without specific authorization, users must not physically or electrically attach any foreign device (such as an external disk, printer, or video system) to OIT equipment or networks.

Unless otherwise guaranteed, users should regard the network communication infrastructure as not secure from invasive technologies. OIT policy will ensure the greatest degree of confidentiality possible. Users may not intentionally conceal their identity when using university computing resources.

Users may not make or attempt any deliberate, unauthorized access to or changes in data on a university computing resource, for example, to read personal communications of other users or to access confidential university files.

Users shall not defeat or attempt to defeat or circumvent OIT security systems, by "cracking" or guessing user identifications or passwords or by compromising room locks or alarm systems.

Users may not intercept or attempt to intercept data communications not intended for that user's access, for example, by "promiscuous" wiretapping.

Users may not deny or interfere with or attempt to deny or interfere with service to other users, e.g., by means of "resource hogging," distribution of computer worms or viruses, etc.

Users are responsible for the security of their OIT accounts and passwords. Any user changes of password must follow published guidelines for good passwords. Accounts and passwords are normally assigned to single users and may not be shared with any other person without OIT authorization. Users must report any observations of attempted security violations.

Unauthorized copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.

