Hixson-Lied College of Fine and Performing Arts
Policy for Use of Information Systems

Hixson-Lied College of Fine and Performing Arts
Policy for Use of Information Systems

Purpose

The use of computers and access to secure electronic information systems has become an essential element in modern education and business. To provide reliable and secure access to these systems, the Hixson-Lied College of Fine and Performing Arts has established the following policies and procedures.

This document operates under the University of Nebraska Policy for Responsible Use of University Computers and Information Systems (Executive Memorandum No. 16). If Policy in this document conflicts with University policy, the University policy shall supersede College policy.

By accepting any account and/or using Hixson-Lied College of Fine and Performing Arts information systems, a user agrees to abide by the College's information systems policies. The College may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of College and University policies or state and federal laws.

When it has been determined that there has been a violation, the College may restrict or prohibit access by an offending party to its information systems through College-owned or other computers, remove or limit access to material posted on College-owned computers or networks, and, if warranted, institute other disciplinary action in accordance with University procedures.

Definitions

For purposes of this document the following definitions shall apply:

a. College refers to the Hixson-Lied College of Fine & Performing Arts and its constituent departments.

b. ITS refers to the Hixson-Lied College of Fine & Performing Arts Information Technology Services office.

c. Information systems refers to computers, networks, server services, software, and other devices that are administered by College Information Technology Services and for which the College is responsible.

Governing Policies of Computing Resources

The College shall adhere to any policy set forth by the University in regards to computers and electronic information systems. This includes, but is not limited to, the following documents:

• Policy for Responsible Use of University Computers and Information Systems (Executive Memorandum No. 16) http://www.nebraska.edu/about/exec_memo16.pdf

• Memorandum on Copyright Law and Compliance http://nebraska.edu/docs/policies/MemorandumonCopyrightLawandCompliance.pdf

• Student Code of Conduct - Section 4.4 http://stuafs.unl.edu/ja/code/index.shtml

If policy in this document at any time conflicts with University policy, policy as set forth by the University shall supersede College policy as outlined in this document.

H-LCFPA Information Technology Services

The College has established Information Technology Services (ITS) within the Dean's Office to provide assistance with information systems. The primary goal of ITS is to support and further the mission of the College through information technology. ITS will seek advice and guidance through the College's technology committee on matters related to the instructional and academic application of information systems with respect to the College's current and long-term goals.

Information Technology Services is responsible for:

- Providing information systems support for academic and business related activities.

- The effective management of information systems within the College by establishing and implementing plans, policies, procedures, and practices that direct the College's information systems investments.

- Assuring the confidentiality, availability, and integrity of College information systems for College faculty, staff, and students.

- Coordinating with the University of Nebraska–Lincoln Information Services whenever possible to maximize efficiencies.

- Representing the College's technology interests to the University.

- Training faculty and staff in the use of College information systems and coordinating with University training resources as needed.

Systems Use

1. The College will adhere to University of Nebraska privacy policy as set forth by Executive Memorandum No. 16 section 7. Below are two key excerpts from this policy.

16.7.A - User Privacy Not Guaranteed

When University information systems are functioning properly, a user can expect the files and data he or she generates to be private information, unless the creator of the file or data takes action to reveal it to others. Users should be aware, however, that no information system is completely secure. Persons both within and outside of the University may find ways to access files. ACCORDINGLY, THE UNIVERSITY CANNOT AND DOES NOT GUARANTEE USER PRIVACY and users should be continuously aware of this fact.

16.7.B - Repair and Maintenance of Equipment

Users should be aware that on occasion duly authorized University information systems technological personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the University deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for University needs. Information systems technological personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

2. Only College faculty and staff, and students who are enrolled in College courses may use College information systems resources. Exceptions may be granted by the College Dean.

3. Each user is responsible for any and all activity initiated on College information systems under his or her user ID and password.

4. Unauthorized access to information systems is prohibited. No one should use the ID or password of another; nor should anyone provide his or her ID or password to another, except in the cases necessary to facilitate information systems maintenance and repairs with ITS. When any user terminates his or her relationship with the University of Nebraska, his or her ID and password shall be denied further access to College information systems. If users suspect misuse of their IDs and passwords, they are required to promptly report that misuse to ITS and reset their password according to current procedures.

5. Use of College information systems for the intention of distributing materials and/or software in violation of copyright is illegal and not permitted.

6. Use of software without a properly obtained license (copied or pirated) is strictly prohibited and illegal under state and federal laws. If ITS finds such software installed on College-owned information systems it will be removed promptly.

7. Enabling file sharing, web services, or other sharing services on a computer greatly increases the security risk of data. For this reason the College prohibits the deployment of these and similar services on College information systems without the approval and assistance of ITS. These services require additional management and therefore a viable need for such services to be provided on individual computers must be met. This is to ensure those services are secure and reliable.

8. Personal use of information systems or electronic communications for non-University consulting, business or employment, except as expressly authorized pursuant to Section 3.4.5 of the Bylaws of the Board of Regents, is prohibited.

9. College information systems are to be used predominately for College-related business. However, under University policy, faculty/staff personal use is permitted so long as it conforms with both University and College policy and does not interfere with College operations or the user's performance of duties as a University employee. Personal use of a University information system to access, download, print, store, forward, transmit or distribute obscene material (as defined by Executive Memorandum No. 16) is prohibited. Personal use is not supported by ITS and may be denied when such use requires an inordinate amount of information systems resources (e.g. storage capacity).

10. No user may monopolize any computer information systems resources, such as disk space, CPU cycles, printer queues, and software licenses. These resources are shared by all users. The use of any information system that interferes with the academic or business pursuit of others is prohibited.

11. In some circumstances users may have access to files that contain data belonging to other users (e.g. collaborative projects). Under no circumstances may a user alter a file that does not belong to him or her without prior permission of the file's owner.

12. Making copies of software having a restricted-use license, and/or circumventing any license or copy protection scheme is considered a violation of copyright and is prohibited.

13. Fair use exceptions exist for instructional purposes. Faculty resources for determining fair use may be found at http://online.unl.edu/Faculty-Resources/Planning/Policies.aspx. Use of copyrighted materials is governed by the Nebraska University Memorandum on Copyright Law and Compliance.

14. Tampering with, circumventing, or disabling any security or management system is prohibited.

15. College information systems and the University network may not be used for the purposes of making unauthorized connections to, breaking into, or adversely affecting other systems on the network, whether these systems are University-owned or not. The ability to connect to other systems via the network does not imply the right to make use of or to connect to those systems unless properly authorized by the owners of those systems.

16. ITS does not support personal computers and/or software for faculty, staff, and students. Resources permitting, ITS may at its discretion provide limited assistance for support of UNL-related business, instruction, or creative activity on personal devices.

17. ITS has the authority to suspend access to any and all College information systems for violations of College and/or University policy, and state and federal laws.

Technology Assets

Inventory

ITS will track information systems assets within the College as necessary to provide efficient support and planning. This includes the recording and archiving of detailed information on every information systems asset owned by the College and its record of service while deployed in the College. These assets will include: desktops, laptops, printers, displays, projectors, software, and other miscellaneous items as determined by ITS. The tracking of additional College property will not be performed by ITS; however, individual schools/departments are encouraged to track additional assets as necessary.

Acquisition

The acquisition and/or installation of computers, software, and/or peripheral devices – such as displays, printers, scanners, or other information systems – should be done in consultation with ITS to ensure compatibility with existing systems, enable effective tracking of College property, and ensure that procurement follows best practices to maximize efficiencies whenever possible. If anyone in the College chooses to independently acquire any such device with University funds, he or she must report the acquisition and all necessary details about the item to ITS so that it may be entered into the College's inventory system. This information is necessary to provide effective maintenance and warranty support. Failure to report the acquisition of equipment greatly increases the difficulty of support and repair by ITS for the asset. Credit card purchases made within the College will be monitored by ITS to ensure that all information systems are properly reported.

Information Systems Disposal and Surplus

Surplus Equipment and Software

The disposition of excess information systems equipment/software must be coordinated with ITS to ensure proper tracking of the asset. ITS will assist the school/department in assessing what can be done with surplus assets. Options include reassignment within the school/department, redistribution among other schools/departments, cost recovery through public auction, or disposal through University surplus.

Destruction of Data

The University requires the destruction of all data on computers and electronic devices prior to surplus or disposal of such assets. Software and data files left on a hard drive or other electronic storage device could potentially be retrieved. This can lead to conflicts with software license agreements and/or result in access to University documents that contain restricted or sensitive information. To prevent this from occurring, any University owned device that has contained files must be delivered to ITS for proper data deletion.

All data devices must be wiped using at minimum a single-pass method before they are repurposed within the College or sent for surplus/disposal. Any data device that is considered to contain highly sensitive data such as financial records or human resources data must be wiped using a minimum seven-pass method before it is to be repurposed within the College or sent for surplus/disposal.

If the device is inoperable and unable to be wiped using conventional methods via data re-writes, the device must be physically destroyed in such a way as to guarantee no data can be salvaged from the device.

Operations and Maintenance

Information Systems Management

The College strives to ensure the confidentiality, integrity, and availability of information stored on College information systems resources by implementing management policies on all College information systems. Such management will help create and maintain a secure and productive environment for the faculty, staff, and students within the college. These policies and procedures shall be appropriate as to provide an environment that is secure and reliable without restricting the ability to freely create, research, and compose academic material.

Services

After consultation between the schools/departments and the Dean, ITS may provide any information service that is necessary for daily operations of academic and business related activities. These services include items such as: calendaring, file sharing, printer serving, technical support, etc. If it is determined that outsourcing of a service would be more economical, ITS will coordinate all activity related to that service to maximize its functionality.

Email

The College will utilize the University-provided email system. ITS will only install and support client software recommended by UNL Information Services. The current supported software for UNL Lotus Notes account users is the Lotus Notes client. The current supported client software for UNL Serve users is Microsoft Outlook and Apple Mail. If an individual faculty/staff member wishes to use an alternate email client, it will be his or her personal responsibility to install and support the software; the University of Nebraska–Lincoln Computer Help Center may be able to provide assistance.

Security

College ITS will follow any security policies and procedures set forth by University Information Services and implement additional policies and procedures as it deems necessary to protect faculty, staff, and student data. This shall include but is not limited to conducting risk analysis and management as necessary on College information systems. The use of secure firewalls, data encryption, requirements for secure/complex passwords, antivirus software, and the implementation of best practices will be necessary for maintaining a safe and secure information systems environment.

Hardware Installation and Maintenance

ITS will perform all installations of College information systems hardware and related devices to ensure proper function, security, and safety. Repairs and/or upgrades to existing information systems hardware will be conducted by ITS. In the event an item cannot be repaired by ITS personnel, ITS may arrange for repair by an outside specialist.

Software Installation and Maintenance

ITS will conduct software installation and routine maintenance, management, and upgrades to College information systems to ensure the security, connectivity, and dependability of all systems. There are numerous security configurations that need to be addressed when installation/upgrades are performed. This includes the installation and upgrading of all major operating system releases: for example upgrading a Mac computer from 10.6.x to 10.7.x or upgrading a Windows computer from Vista to Windows 7.

Labs and Studios

Information systems are provided for use by faculty, staff, and students to support the mission of the College. Access to these systems is a privilege. Users are responsible for using these resources in a respectful manner.

Management of Instructional Spaces

It will be the responsibility of each school/department to maintain and develop its own respective information systems in regards to classrooms, labs, studios, and equipment that is available for checkout. Any school/department that makes resources available for check out to faculty, staff, and students must keep a detailed inventory of all such equipment and track its use while checked out. If the school/department does not have adequate resources to manage an instructional space, arrangements can be made between the school/department and the Dean to coordinate management of the space with ITS.

ID Management

Passwords should be difficult for others to guess or break. For this reason the College will use University standards for establishing a secure password. See https://id.unl.edu for additional information.

Password Requirements

- Must be between 8 and 127 characters in length.
- Must not contain your: account ID, email, last name, first name, full name, or similar attributes.
- Must meet at least 3 of the 4 following conditions:
    1. Contain at least 1 numeric character
    2. Contain at least 1 special character, ie: ~ ! @ # $ % ^ & * ( ) _ + = - ` { } [ ] | \ : " ; ' < > , . ? /
    3. Contain at least 1 uppercase letter
    4. Contain at least 1 lowercase letter

If a user suspects misuse of their ID and password, he or she is required to promptly report that misuse to ITS and reset their password as necessary with current procedures.

Network Connections

The College will utilize the University-provided network for both wired and wireless network access. Any networkable information system or other capable device must be registered with University Information Services in accordance to their current guidelines to ensure a reliable and secure connection.

University of Nebraska–Lincoln Information Systems policy prohibits the creation of any wireless network on University property. Users are prohibited from creating any such personal or group-related networks without the consent and assistance of ITS and University Information Services. This includes enabling a computer, cell phone, or other mobile device to create a "hotspot" offering wireless connections.

Back Up

Individual Back Up

Backing up data should be considered an essential maintenance task by all users. At this time individual computers and workstations are not centrally backed up by ITS. Individuals are encouraged to find a means by which to back up their data, whether by personally undertaking the task or asking their respective school/department for assistance. Acceptable methods for backing up data include directly attaching a secondary storage device such as an external hard drive that can be placed in a safe location, or subscribing to an online back up provider such as the University-hosted NSave system, or other third party systems. ITS will provide assistance for any user who would like to set up a back up routine for their College computer.

ITS does not recommend the use of flash memory based devices such as USB flash drives or SD cards for back up due to their limited write life span and high-failure rate.

ITS Hosted Environments

ITS, in conjunction with College schools/departments, will maintain backups of any hosted system that is considered mission critical to the continuing operation of the College. These backups are for recovery of the systems in the case of system failure or major disaster due to flooding, fire, etc. and are not intended to be used for the restoring of deleted files due to user error. If ITS is unable to provide backup for any of its hosted services, ITS will notify the affected users that any information kept on that system is subject to loss.

Notification

This Policy shall be published in all staff and faculty handbooks and student catalogs, and placed on College ITS web sites in order to fully notify users of its existence.

Application and Enforcement

This Policy applies to all faculty, staff and students in the Hixson-Lied College of Fine and Performing Arts. Each school and department is encouraged to provide supplemental policy guidance, consistent with this Policy, designed to implement the provisions herein. Each school/department shall cooperate with ITS and the University in enforcing this Policy in a manner best suited to its own unit. It is expected that enforcement will require cooperation between such departments as ITS, human resources, affirmative action, academic affairs and student affairs. Prior to any denial of access or other disciplinary action, a user shall be provided with such due process as may be recommended by the University's Office of the General Counsel.