

GUIDELINES FOR THE USE OF INFORMATION TECHNOLOGY RESOURCES

Information Technology Services

INFORMATION TECHNOLOGY RESOURCES

Information technology (IT) resources at UNK include computers, mobile devices, storage devices, peripheral devices, supplies, software, documentation, networks, services, and support.

UNK is a provider of a means to access the vast amount of information available through electronic resources, but is not a regulator of the content of that information and takes no responsibility for the content, except for that information the University itself and those acting on its behalf create.

UNK cannot and does not guarantee user privacy. Users should be aware that on occasion duly authorized personnel have authority to access individual user files or data in the process of performing repair or maintenance of equipment. Users should also be aware that the Nebraska public records statutes are very broad in their application and some University records contained in electronic form require disclosure if a public record request is made.

PERMITTED USE

Accepting any account and/or using UNK's IT resources shall constitute an agreement on behalf of the user to abide by these Guidelines. Access to IT resources at UNK is a privilege, not a right, and must be treated as such by all users. Failure to act in accordance with these guidelines and relevant local, state, and federal laws and regulations may result in denial of access to IT resources or other disciplinary action.

IT resources are to be used predominately for University-related business. However, personal use is permitted so long as it conforms with these Guidelines and does not interfere with University operations or an employee user's performance of duties as a University employee.

MISUSE OF INFORMATION TECHNOLOGY AND NETWORK SYSTEMS

Misuse of University IT and network systems is prohibited. Misuse includes the following:

- A. Attempting to modify or remove IT equipment, software, or peripherals without authorization.
- B. Accessing without proper authorization computers, software, information, or networks to which the University belongs, regardless of whether the resource accessed is owned by the University or the abuse takes place from a non-University site.
- C. Taking actions, without authorization, which interfere with the access of others to information systems.
- D. Circumventing logon or other security measures.
- E. Using information systems for any illegal or unauthorized purpose.
- F. Personal use of information systems or electronic communications for non-University consulting, business or employment, except as expressly authorized by Section 3.4.5 of the Bylaws of the Board of Regents.
- G. Sending any fraudulent electronic communication.
- H. Violating any software license or copyright without the written authorization of the software owner.
- I. Using electronic communications to violate the property rights of authors and copyright owners.
- J. Using electronic communications to harass or threaten others, so as to interfere with the educational or employment experience.
- K. Using electronic communications to disclose proprietary information without the explicit permission of the owner.
- L. Reading other users' information or files without permission.
- M. Academic dishonesty.
- N. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records.
- O. Using electronic communications to hoard, damage, or otherwise interfere with academic resources available electronically.
- P. Using electronic communications to steal another individual's works, or otherwise misrepresent one's own work.
- Q. Using electronic communications to fabricate research data.
- R. Launching a computer worm, computer virus or other rogue program.
- S. Downloading or posting illegal, proprietary or damaging material to a University IT resource.
- T. Transporting illegal, proprietary or damaging material across a University network.
- U. Violating any state or federal law or regulation in connection with the use of any IT resources.
- V. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material.
- W. Using another's ID or access codes without permission of the appropriate System Manager.
- X. Creating a web page or similar service using or attached to UNK IT or network resources that does not comply with UNK's Web page guidelines.

ENFORCEMENT

The Assistant Vice Chancellor for Information Technology is authorized to monitor the use of all campus-wide IT resources and Department and Program Administrators are authorized to monitor their specific IT resources, to manage and protect those resources and the rights of their users, and to recommend the imposition of sanctions against any person who violates these guidelines. Sanctions may be both internal, involving loss of IT privileges or other university disciplinary measures, and external, involving civil or criminal action under the Nebraska Computer Crimes Act or Federal Statutes.

08/13/2015

Date of Change	Responsible	Summary of Change
August 2015	ITS Policy Team	Updated name of Office of Residence Life. Standardized format.