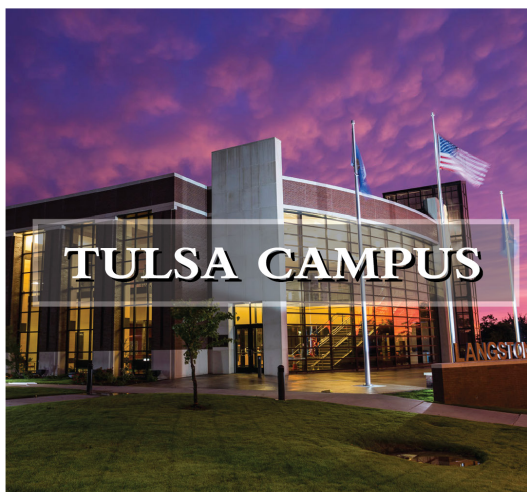# TRI-CAMPUS STUDENT TECH GUIDE
2015-2016

Langston Campus

OKC CAMPUS

TULSA CAMPUS

Contact Us
p.13

Hours
of
Operation
p.13

Table of Contents

Help Desk Tech Support & Resource Center Services

The Helpdesk provides services in the following areas of technology:

- PC Diagnostics
- PC software installation
- Client Imaging and Server/Client deployments
- Campus Network Logins
- Navigation of the campus website
- Creating email accounts
- Other institutional and/or departmental wide software applications (Physical Therapy, College of Education, etc.)

The Resource Center will provide the following services:

- Allowing faculty, staff, and student organizations to check out screens and projectors

Individuals may not use technology equipment without proper approval from the requesting department or CIO.

Individuals may not use another user's computer account or user I.D. or change another user's password.

Users are responsible for their use of computer hardware, software, accounts, user I.D.s and passwords.

Users are personally responsible for all resources assigned to them.

Student Information Systems

Through the SIS, individuals may check grades, schedules, obtain an unofficial transcript, verify the status of financial aid, etc. To access the SIS:

- Place cursor over **Student Life**
- **Student Information Systems** is listed under the **Online Support** heading.
- Your "Student ID" is your Campus-Wide ID. (Your SSN will also work.)
- Your PIN is your 6-digit birthday i.e. 010183
- You will then be prompted to change your PIN to a different 6-digit number and log in again with that new PIN
- Please do not forget this PIN. **If you have login issues please call ext. 3225 from a campus phone or 466.3225 from off-campus.**

Downloading and Software Piracy Policy

Duplicating copyrighted videos, music, or software programs without permission of the author is broadly defined as copyright infringement. The illegal activity of duplicating, using, selling or distributing copyrighted material is equivalent to theft and is therefore a crime. Unauthorized installation of software is stealing and is also illegal.

Possession or use of pirated software also makes one potentially liable for piracy.

The maximum penalties are $250,000 in fines and up to five years in prison. Ignorance is not an excuse.

All of us have a responsibility to say "no" to software piracy. Purchase and use only legal copies of software with serial numbers.

If you suspect the occurance of piracy, you should report information to ITS at 405.466.3215. Your identity will be held in confidence.

Legal Downloads

There are legal download alternatives. Access the list of legal resources for legal downloading of copyrighted material by logging on to:
http://www.educause.edu/legalcontent

Reporting a Cable, Phone, or Internet Problem

• Go to your apartment's Main Office (Club House) and fill out the "ITS Reported Problems" form; ITS obtains these forms every Tuesday and Thursday and will complete the requests within that week.
• We will contact you to schedule a visit for your technical problem.
• You may also submit a request online following this path: **Faculty & Staff** » **Online Support** » **Information Technology Services** » **HelpDesk Request Form**

Problems With Your Personal Computer

• ITS employs technicians that can either fix or tell you what problems you have with your machine; they are available in **Gandy Hall**.
• There may be a cost to repair your machine; personal computer repair is not a function of the ITS department. Please consult with the technician concerning any fees he or she may charge.

Accessing Library Sources on the Internet

• You may log in by entering the first four letters of your last name.
> i.e. John Doe = doej
> > John O' Doe = odoe
> > John O-Doe = odoe
• Then enter the last four numbers of your social security number.
> i.e. 123456789 = 6789
• **Please contact ITS for login issues at extension 3500 from a campus phone or 466.3500 from off-campus.**

Accessing D2L for Online/Hybrid Courses

• You must first activate your LionKey account by clicking on **Logins** in the top right corner of the homepage.
• Click on **Activate LionKey**
• Enter the first two letters of your last name
• Enter the last five digits of your Social Security Number
• Enter your date of birth
• Follow the direction on the activation wizard paying close attention to the details of setting up your encrypted password.
• Allow 5-30 minutes or more for your account to be fully activated.

Accessing D2L for Online/Hybrid Courses (cont.)

Once activated:
- Return to the **Logins** link
- Click on **Desire2Learn**
- Enter your Username and Password obtained through the LionKey activation process.
- Once logged in, you should be able to see your courses.

For help, call 405.466.2008.

How To Log On To Your Email Account and Your University Computer

You may login to campus computers and your langston.edu email with the same username and password. Your username is created upon your acceptance to the University and consists of the first initial of your first name, the first initial of your middle name (if applicable), your last name and the last 4 digits of your student ID number. Your initial password consist of your eight (8) digit birthday and should be changed. i.e. 01011983

*For email, go to **http://exchange.langston.edu/** and enter the above information.

How To Change Your University Email Password
- Go to **http://exchange.langston.edu**
- Log in using your email password and username.
- Select the *Options* tab located at the top right corner of the window (below your name).
- Select *Change Password*.
- Fill in current and new information.

Student Logins Portal
- You may access a variety of student-related pages through the **Logins** link located in the top right corner of the Website. Herein you will find access to the SIS system, your campus email, D2L as well as activation of your LionKey account.

Computer Labs on Campus - Langston Campus
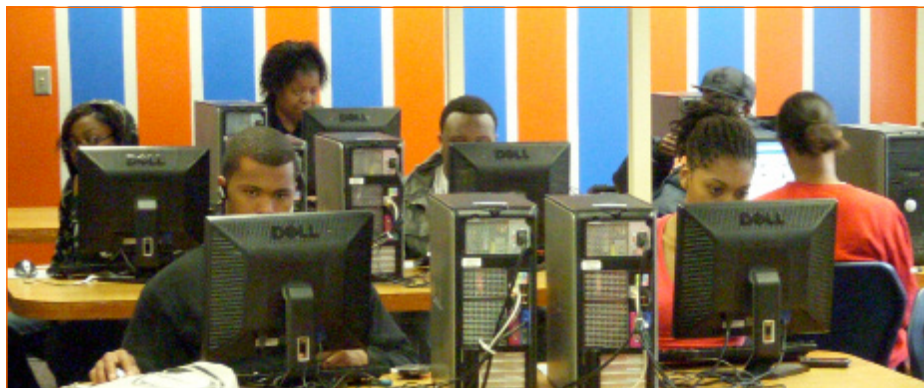
- **G. Lamar Harrison Library**
  M-Th, 8am-9:45pm;
  Fri 8am-4:45pm;
  Sat 9am-5pm
  Sun 2pm-9:45pm
- **Moore Hall**
  Room 209 - Business**
  Room 211 - Business**
  Room 312 - Programming**
- **Hamilton Hall**
  Room 115 - Technology**
  Room 204 - Biology**
  Room 318 - Chemistry**
- **Jones Hall**
  Room 104 - Writing**
  Room 205 - Math**
  Room 215 - Math**
- **Sanford Hall**
  Room 217W - Education**
  Room 318 - Journalism**

- **C.F. Gayles Gymnasium**
- Room 301 - Athletics**
- **Physical Therapy**
  Room 117 - Physical Thera-
  py**
- **University of Women**
  Room 310
- **Hargrove Music Hall**
  Room 104 - Music**
- **Student Apartments**
  Commons Office
  Centennial Office
  Scholars Office
- **Gandy Hall**
  Room 208 - Upward Bound**
- **Allied Health**
  Room 216 - Nursing**
- **Agriculture Complex**
  Room 402 - AutoCAD/GIS**

**These computer labs are for use by students in this major.
  Contact your advisor or professors for more information.

Computer Labs on Campus - OKC Campus

There are two computer labs at the Oklahoma City campus.
• Main Computer Lab Room 107
Available for all students
• 24/7 Computer Lab Room 114
Access for Graduate Students only; any day and time during the school semester. At the end of each semester, access is deactivated.
Contact your advisor or professors for more information.

Computer Labs on Campus - Tulsa Campus

• OSU Nursing - Tulsa Campus
• Media Center - Classrooms
Rooms 209, 210, 213
**These computer labs are for use by students in this major.
Contact your advisor or professors for more information.

University ID Card

The Langston University ID Card is equipped with many useful features. Students may use their card to gain entry into campus events and activities. Attendants of the Langston Campus may use their card in on-campus food/vending areas. In the near future, cards may also be used for campus Laundry and Copy services.

DO NOT SHARE YOUR CARD WITH ANYONE - Doing so may result in confiscation of the card and an academic misconduct report may be filed against you. You should treat your card like any other card of value to you.

Tips:
- Always keep in a safe, clean place
- If dirty, clean with a lint-free cloth dampened with isopropyl alcohol (rubbing alcohol)
- Do not bend, deform, or write on your card.
- Do not expose your card to high temperatures or direct sunlight.
- Keep your card dry.
- Following these tips will prevent you from damaging your card and having to purchase a new one.

University ID Card Problems:

What if I lose my card?
- Langston Campus students may contact Dr. Natasha Billie, Dean of Student Services, in the Student Affairs Office. If you attend the OKC or Tulsa campus, please notify the Office Manager or Front Desk.
- *I lost my card, paid and received a new one, then found my old one. Can I reactivate the old one?*
    No. Once a new card has been issued, your old ID card can never be reactivated.

Connecting to the Internet

- All student apartments are now equipped with full, wireless internet service. Connection is achieved through each living facility's individual SSID eg. Centennial Court - Centennial Students, The Commons - The Commons, and Scholars Inn - Scholars Students. For assistance with any issues, please contact the HelpDesk or (405) 466-3205.
- On-campus WiFi is accessed through the Langston Lion Open portal or LU Wireless Open; simply click to connect.

Registering for Campus Alerts

The Campus Alert system provides alerts via text message and/or email when there is a campus warning. To register:

- Click on the Logins link at the top right of the home page.
- Your username is that which you use for campus computers and email (generally speaking, the first initial of your first name, the first initial of your middle name, your last name, and the last 4 digits of your student ID number).
- You must create a password that is at least 8 characters long and contains at least 1 upper case letter.
- Click Register and follow the remaining prompts.

Dell/Langston Partnership

This partnership will allows LU students, faculty and staff to purchase DELL equipment at a reduced price. To take advantage, follow these steps:
- Type http://www.delluniversity.com
- Click on "Get Started"
- Select your classification
- Select your school
- Type in your lunet.edu e-mail address.
- A confirmation e-mail will be sent to your lunet.edu account.
- Click on the link in the e-mail to take you to the Langston/Dell store page and follow the directions from there.
Please call ITS (466.3500) with questions.

Acceptable Use Policy

A. Introduction

Langston University (LU) attempts to create an environment where university information technologies meet the needs of university programs in research and instruction.

As an institution of higher learning, LU encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. Consistent with other University policies, this policy is intended to respect the rights and obligations of academic freedom, while protecting the rights of others. The computing and network facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. Usage of these facilities is a privilege rather than a right. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet. The following statements address, in general terms, the University's philosophy about computing use.

B. Scope

This policy is applicable to all individuals using University owned or controlled computer and computer communication facilities or equipment. It is applicable to all University information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the University. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines and/or restrictions. Such policies may not relax or subtract from, this policy. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for securing appropriate authorization (Per 2-0501 Administrative Information Systems policy) and to furnish Information Technology Services (ITS DEPARTMENT) with a copy of the approved document. Units must also publicize both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the unit administrator shall provide the Chief Information Officer's office with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

C. Authorized Users

An ITS DEPARTMENT computer systems account is created for all regularly enrolled LU students. Accounts are valid as long as a student is enrolled at LU. An authorized user is any person who has been granted the privilege by the University to access ITS Department computing and network systems and whose usage complies with university policy. Authority to use a particular University computing or network resource should come from the campus unit responsible for operating the resource.

D. Authorized Use

Use of University computers must comply with US Government Federal and State laws and University policies. Facilities and accounts are to be used for the activities for which they are assigned.

Users are held responsible for their own computer accounts and the usage thereof.
Computing facilities, services, and networks may not be used in connection with compensated outside work for the benefit of organizations unrelated to the University except in connection with scholarly pursuits (such as faculty publishing activities). State law generally prohibits the use of University computing and network facilities for personal gain or profit, and use of computing resources for unauthorized commercial purposes, unauthorized personal gain, or any illegal activities is prohibited.

E. Privacy

Following LU Policies and Procedures, Oklahoma laws and applicable federal laws, LU strives to protect personal privacy and confidentiality. Information will be handled with the strictest of security and confidentiality standards.

(Buckley Amendment – Family Rights and Privacy Act, Open Records Act, Federal Electronic Communication and Privacy Act of 1986, Federal Computer Intrusion Laws)

F. User Responsibilities

University policy, ethics and etiquette are required to successfully participate in the LU community and are extended to the computing environment. Individuals who share computing resources at LU and who also use those resources to access the worldwide network (Internet) are responsible for knowing and following the Appropriate Computer Use Policy. It is the responsibility of the user to access and use data in accordance with the university's policy and applicable state and federal laws.

Access to the information resource infrastructure both within and beyond the University campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at LU is a privilege granted to University students, faculty, staff, and affiliates who have been granted special permission to use such facilities. Access to University information resources must take into ac

count the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the University.

Anyone who accesses, uses, destroys, alters, or damages University information resources, properties or facilities without authorization, may be guilty of violating state and/or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this Policy to disciplinary action by the University, including possible termination from employment, expulsion as a student, and/or loss of computing systems privileges.

Individual users certify understanding and agreement to adhere to LU's policies by signing on to LU systems. Specifically, an employee acknowledges an understanding of and agreement to adhere to the following:

* Users are personally responsible for all activities on their User ID or computer system and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.
* Updates to the system and changes in system data are to be made in a manner that is consistent with the University's policies and procedures which govern the particular action to be changed.
* Computing resources are to be used only for legitimate University business.
* It is against the University's policy to use the University's records including, but not limited to, confidential information for personal interest or advantage.
* Proper password security is to be maintained by not revealing passwords to anyone.
* Security is to be maintained by not providing anyone access to or use of the University's information systems.
* Proper physical security is to be maintained by not leaving a workstation/terminal/laptop unattended while logged into the University's systems.
* The privacy and confidentiality of all accessible data is to be maintained and it is understood that unauthorized disclosure of personal /confidential information is an invasion of privacy and may result in disciplinary, civil and/or criminal actions against an individual.
* Suspected security violations will be reported to the ITS DEPARTMENT for investigation.
* Under existing law, any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data may be charged with a felony.
    The University also requires that members of its community act in accordance with these responsibilities,
* Act in accordance with the Family Educational and Privacy Rights Act (Buckley Amendment),
        o Respect copyrights and licenses,
        o Respect the integrity of computer-based information resources,
        o Refrain from seeking to gain unauthorized access,
            o Refrain from games
        o Respect the privacy of other computer users, and to comply with this Policy, the University's Student or Faculty Handbook, as appropriate, LU Policies and Procedures, relevant laws and contractual obligations, and the highest standard of ethics. LU accommodates and does not interfere with standard technical measures used by copyright holders to identify and protect their rights (for further information see the U.S. Copyright Office at http://www.copyright.gov/).

The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Usage is a privilege, not a right.

Users are held responsible for their own computer accounts and the usage thereof. Users will be subject to disciplinary action, including termination and/or loss of privileges for misuse of computers or computing systems under their control.

Business units and individuals may, with the permission of the ITS Department Director and where deemed necessary, approval from the Chief Information Officer (CIO) in consonance with applicable University policies and guidelines, configure computing systems to provide information retrieval services to the public at large. However, in so doing, particular attention must be paid to University policies regarding authorized use. Usage must be consistent with the mission of the University, including ownership of intellectual works, responsible use of resources, use of copyrighted information and materials, use of licensed software, and individual and unit responsibilities. Contact information for the system administrators of these systems must be reported to the ITS Department.

G. Special Notifications
The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be the recipients of materials they find offensive. Those who use e-mail and/or make information about them available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information. Personal use of any University information system to access, download, print, store, forward, transmit or distribute obscene material is prohibited. The University's computing and network systems are a university owned resource and business tool, only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the University. The University owns everything stored in ITS Department systems unless it has agreed otherwise. The University has the right of access to the contents of stored

computing information at any time for any purpose for which it has a legitimate "need to know." The University will make reasonable efforts to maintain the confidentiality of computing information, storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of said contents.

The LU Data Communications Network is a mission critical strategic University resource. In order to protect the Data Communications Network, devices that are considered end nodes, other than computers/printers/copier/scanners, and workstations must not be plugged into any network port, unless special arrangements are made with ITS DEPARTMENT and approved by the ITS DEPARTMENT Director or where deemed necessary with the approval of the Chief Information Officer (CIO). This includes but is not limited to hubs, switches, repeaters, routers, network modems, servers and wireless access points whose installation have not been coordinated and registered with ITS DEPARTMENT. These devices may be incorrectly configured or incompatible with the LU Network causing outages and reliability problems to all or part of the network. Devices not approved for use on LU's Data Communication Network will be disabled to ensure the stability and availability of the network.

Devices not approved for use on LU's Data Communication Network will be disabled to ensure the stability and availability of the network

ITS DEPARTMENT strives to provide high availability and stable network resources relevant to the LU community's needs. Colleges or Departments needing additional network resources should contact the ITS DEPARTMENT Help Desk.

H. Access
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. A password should never be shared, not even with computer support personnel. Users are personally responsible for all activities on their User ID or computer system, including security of their own passwords and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.

I. Ownership and Rights of Access to Software and Data
LU has software and data that have been acquired through a variety of sources. Some software and data, though available for use by all users of LU's systems, remain the property of the supplier and the dissemination of the software or data (in any form) is strictly prohibited. This also applies to software made available by non-ITS DEPARTMENT University personnel. This software is not to be distributed, unless authorized by the person or department that initially secured the software or data. No software or data should be distributed, reproduced or used without ensuring that proper licensing and/or authorization has been obtained.

J. Conduct Expectations and Prohibited Actions
LU provides computing resources and worldwide network access to members of the LU community for legitimate academic and administrative pursuits. ITS Department to communicate, access knowledge, and retrieve and disseminate information. All members of the LU community (faculty, staff, students, and authorized guests) sharing these resources also share the rights and responsibilities for their use.

Examples of misuse include, but are not limited to:

   * Knowingly running or installing on any computer system or network, or giving to another user, a program intended solely for the purpose of damaging or placing excessive load on a computer system or network. This includes, but is not limited to, computer viruses, Trojan horses, worms, bots, flash programs or password cracking programs.
   * Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the system administrator. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data.
   * Using computers or electronic mail to act abusively toward others or to create a hostile environment, violent reaction, such as stalking, threats of violence, or other hostile or intimidating "fighting words."
   * Posting on electronic bulletin boards or web pages materials that violate the University's codes of conduct (faculty, student). This includes posting information that is slanderous or defamatory in nature or displaying graphically disturbing or sexually harassing images or text in a public computer facility or location that are in view of other individuals.
   * Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
   * Using campus networks to gain, or attempt to gain, unauthorized access to any computer system.
   * Using a computer account or obtaining a password without appropriate authorization.
   * Masking the identity of an account or machine. This includes sending mail that appears to come from someone else.
   * Performing an act without authorization that will interfere with the normal operation of computers, terminals, peripherals, networks, or will interfere with others' ability to make use of the resources.
   * Using an account for any activity that is not approved through policy and procedure, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain.

K. Systems Security Officer
The person designated by the Chief Information Officer, shall be the primary contact to work in conjunction with appropriate university officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concern

ing law shall be referred to Legal Counsel for advice and action as applicable.

In situations that are an immediate threat to the security or operation of a computer or network, the ITS Department may require immediate intervention of access privileges and affected user files or messages. In such an emergency, the ITS DEPARTMENT will notify, as soon as possible, the appropriate university administrators and users affected by the situation.

L. Consequences of Misuse

Misuse of computing, networking, or information is unacceptable, and users will be held accountable for their conduct. Serious infractions can result in temporary or permanent loss of computing and/or network privileges and/or Federal or State legal prosecution. Appropriate corrective action or discipline may be taken in conformance with applicable personnel policies and student policies. Some computer abuses are a crime, (such as illegal reproduction of software protected by U. S. copyright law) and penalties can include a fine and/or imprisonment.

Abuse of computing privileges is subject to disciplinary action, including termination of employment. If system administrators have strong evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

* Notify ITS DEPARTMENT.
* Notify appropriate departmental administrators
* Will notify the user's instructor, department or division chair, or supervisor of the investigation, when appropriate.
* May suspend or restrict the user's computing privileges during the investigation.
* May inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media.
* Will refer issues, when appropriate, to the appropriate University department for possible disciplinary action, i.e., this may include but not be limited to the Office of the Chief Information Officer, the Office of the Vice President for Student Affairs, the unit administrator for staff, and the Dean of the School for faculty.

Users, when requested, are expected to fully cooperate with system administrators and / or the ITS DEPARTMENT regarding any investigations of system abuse. Failure to cooperate may be grounds for cancellation of access privileges or disciplinary action, including dismissal.

When individual privileges to access University computing resources have been suspended, a user may request that the Information Technology Services Director, or his/her designee, review the suspension. The Information Technology Services Director, or designee, in his/her discretion, may reinstate privileges, alter any restrictions that have been imposed, or refuse to interfere with the administrative action taken at that time. Further appeals may be filed with the Office of Student Affairs, the University Personnel Office, or the Chair of the Faculty Council, as appropriate.

Failure to comply with these policies, rules and regulations may result in disciplinary action, up to and including dismissal. Any violation of local, state or federal laws may carry the additional consequence of prosecution under the law, where judicial action may result in specific fines or imprisonment, or both; plus the costs of litigation or the payment of damages or both; or all.

M. Notification

References to this policy will be in the LU Catalog, the Student Rights and Responsibilities policy, the ITS DEPARTMENT web site and the LU Policies and Procedures Letters.

N. Application and Enforcement

Each University campus shall be responsible for enforcing these Policies in a manner best suited to its own organization in compliance with those established by the University's ITS Department. It is expected that enforcement will require cooperation between such departments as computer systems administration, personnel, affirmative action, academic affairs and student affairs.

Contact Us

The ITS Department may be reached via the following numbers:

- Langston Campus (Calvin Hall): (405) 466-3215
- OKC Campus: (405) 530-7500
- Tulsa Campus: (918) 877-8143

All ITS Departments are open Monday - Friday from 8:00AM to 5:00PM.