LUPANE STATE UNIVERSITY

Lupane State University ICT Policy

P O Box AC 255, ASCOT, BULAWAYO

ZIMBABWE

www.lsu.ac.zw

Lupane State University ICT Policy

Date effected : ……/……/……

Date Last Updated : ……/……/……...

Information Communication Technology and Services Policy

1. Definition of terms

i. Where the terms “Lupane State University”, “University” or “LSU” are used, they will refer to Lupane State University and its associated locations.

ii. The term “ICT” refers to any communication device or application, encompassing: computer and network hardware and software, satellite systems, and so on, as well as the various services and applications associated with them.

iii. The term “user” refers to any person who accesses an ICT system, service or equipment owned, managed or supplied by LSU.

2. Preamble

Information Communication Technology and Services department (ICTS) is the hub that supports the day to day operations of the institution. The ICTS department is not ignorant of the challenges regarding ICT security and the provision of guidelines for acceptable use of ICT resources as well as legal compliance. This ICT Policy document seeks to provide guiding principles that ensure compliance, acceptable and secure use of information communication technology by the LSU community.

3. Objectives

- Improve and promote efficient use of information systems.
- Enhance information security systems at LSU.
- Augment availability of ICT systems.
- Develop a sense of awareness, co-operation, trust and consideration for others.
- Prevent bad publicity and putting the name of the university into disrepute.
- Curb fraudulent activities.

4. Scope

The ICT policy document relates to all Information Technology facilities and services provided by LSU's ICTS department including, but not limited to, email system, databases, integrated systems, operating systems, internet, telephone systems, wireless communication, printers and copiers. All LSU employees, volunteers, students and attachés are expected to adhere to it. This document will be effective from the date of approval by the Senate committee.

A deliberate breach of this policy will lead to disciplinary measures being taken against the offender through existing staff or student disciplinary procedures which may include being denied access to computing facilities.

Staff and Students must comply with the following:

4.1 Copyright: Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.2 Do not attempt to gain unauthorised access to information or facilities. It is an offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information resources you feel you need, contact the ICTS department.

4.3 Disclosure of personal system passwords or other security details to other staff members is not allowed. The user shall be liable for any information security breaches that were conducted using their password (s) .If someone else gets to know your password, ensure you change it or get ICTS support to help you.

4.4 ALWAYS check external removable disks for viruses, even if you think they are clean.

4.5 Do not access, publish, bookmark or download obscene or pornographic material.

4.6 The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety is prohibited.

4.7 Do not use the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).

5 Email

This section governs the use of the University's e-mail system to facilitate the exchange of electronic information both internally and externally in the institution. It is important to note that the University's e-mail system is a key communication system within the institution. Inappropriate use of the e-mail system can lead to virus infection, which ultimately lead to degradation of network performance, or in extreme circumstances could take the whole of the University network down.

5.1 Computer Viruses

Incoming and outgoing e-mails and their attachments may carry dangerous or potentially business damaging viruses. If an individual is in any doubt about the contents of an e-mail message and suspects the existence of a virus they should not open it, but must consult the ICTS department immediately to obtain technical assistance. If there is any doubt regarding e-mail attachments, the ICTS department should be contacted immediately.

You will :

- be responsible for all electronic mail originating from your User ID;
- not forge, or attempt to forge, electronic mail messages;
- not attempt to read, delete, copy or modify the electronic mail directed to other users without prior consent;
- not send, or attempt to send, harassing, obscene and/or other threatening e-mail to

a user of any e-mail service;

- not send 'for-profit' messages or chain letters.

5.2 Offensive or obscene e-mail

If there is any reason to suspect that an incoming e-mail may contain offensive or obscene material, where possible, refrain from opening it. Under no circumstance should the e-mail be sent on to another user, and it should either be reported to the ICTS department, or deleted immediately. Never send via-email pornographic or other any offensive materials that contravene University Policy. Employees are required to report inappropriate use of e-mail to the ICTS department.

5.3 Confidentiality

E-mail communication is not always a secure means of communication across the internet. Be cautious when sending strictly confidential or commercially sensitive messages through theInternet since these cannot be guaranteed. Employees shall have no expectation of privacy in anything they store, send, or receive on the institution's email. ICTS may monitor messages without prior notice. ICTS is not obliged to monitor email messages.

5.4 Content

E-mails should not be treated as an informal means of communication. Always use professional language when e-mailing internally or externally, so the same care should be given to the tone and content of e-mails as with paper communication.

5.5 ICTS department Emails

The ICTS department is ultimately responsible for the institution's network configuration, maintenance, repair and upgrade of Information Systems. As part of its system-wide responsibilities the ICTS department will communicate changes to the network which may make network resources unavailable for short periods of time during working hours and will communicate upgrade information which may require certain actions on the part of network users; will alert system-users to virus threats; and, provide other information it deems useful to

members. As the ICTS department we are aware that there might be downtime during working hours as a result of network failure beyond our control e.g. ISP network problems, these will be communicated in time. Users should not auto delete emails from ICTS before reading them, it is their responsibility to read and act upon these communications. If any clarification is required the department may be contacted and it will accommodate those needs.

6 Internet

The main aim of this section is to provide advice and guidance, to create a safe and secure environment for staff and students when undertakaking University business and research over the Internet.

Using the Internet for any illegal activity, including violation of copyright or other legal rights, the unauthorised transmission or receipt of proprietary information, or transmitting any material that is in breach of Zimbabwean government legislation, is not allowed. In addition, the Internet should not be used for the transmission, retrieving, observing or storing of any communication that (is):

i. Discriminatory or harassing in any sense whatsoever and whether prohibited by the law or not;
ii. Pornographic or derogatory to an individual or group;
iii. Involves accessing entertainment, sport or gambling websites or other websites which have no legitimate connection to the University's business;
iv. Defamatory or threatening, whether legally actionable or not;
v. Illegal or contrary to the university's policies or business interests;
vi. The ICTS department reserves the right to add or delete services as the institution's need changes or conditions warrant.

6.1 Safeguarding Access to Workstations

Workstations should not be left unattended as this provides an opportunity for others to access personal documents and the e-mail system and send items in one's name. A password screensaver should be used to prevent unauthorised access. All network users are issued with a

unique username and password which must be changed at regular intervals and is confidential to the user.

7 Equipment movement / loans

The ICTS department is the custodian of all university ICT equipment and software. No equipment or software may be borrowed without permission from the ICTS Manager or Director. Security is authorised to stop and question any person seen leaving LSU premises with ICT equipment or software. An application for removal of university equipment form must be filled and signed by the Security officer, Asset register and ICTS Director or Manager before ICT equipment is taken out. The form must be filled in triplicate.

8 Hardware

Desktop computers will be Personal Computer (PC) based, except where there is a good reason or an appropriate business case to use an alternative platform. All computers and associated accessories will be sourced from a reputable supplier in liaison with LSU's Buying section.

All computers and associated devices such as printers, scanners, routers etc used on the University network, should be registered in the university ICT's inventory.

8.1 Software

ICTS department will endeavor to use open source to reduce expenditure on licencing where possible.

The principles that underpin the purchase of software are:

i. Sound academic or administrative rationale
ii. Compatibility and durable use for a long time
iii. Value for money

9 Training ICT staff

The department will periodically train ICTS staff so that the department is abreast with latest ever changing technology.

10 Outreach

The department shall be engaged in community outreach work in providing computer literacy training and also helping local communities and schools setting up ICT infrastructure.

11 Student accounts

LSU encourages students to be familiar with the use of Information, Communication and Technology Services (ICTS) to benefit their learning. When student accounts have been activated, students are responsible for everything that occurs on their account:

- Logon passwords must be kept confidential;
- Students must not attempt to gain unauthorised access to secured network resources or another user's account;
- Report any security lapses/concerns to the ICTS department.

11.1 Computer rooms and ICT hardware usage

- Rooms containing ICT hardware may only be entered if a staff member is present.
- Bags must remain outside the computer rooms.
- Food and/or drinks are not to be brought into computer rooms.
- Computer equipment must not be swapped around (e.g. changing of keyboards, mice from one computer to another).
- Students must not attempt to access the inner working of a computer or ICT device outside normal use.
- All equipment faults and/or damage must be reported to the ICTS department immediately.

11.2 ICT Usage

- All ICTs, including local area network, Wireless Local Area Network, Internet and email are to be used for LEARNING PURPOSES.
- Playing of software games or downloading inappropriate content is prohibited.
- Students must adhere to the laws concerning piracy, copyright and other intellectual property rights.

- It is illegal to retrieve, view, post, store, or distribute pornographic, obscene, violent or offensive material through the university's email, network or hardware.

11.3 Student's email

As the university invests in servers, students will be provided with an LSU email account. This account will be used for sending educational notices to students and for general communication.

12 Finance

The ICTS department plays a central facilitation role to all departments helping them fulfill their mandates and therefore its funding affects all departments. The university must set aside a certain levy on students' fees for continual development and improvement of the university's ICT infrastructure.

13 Policy Maintenance & Review

- Periodic reviews may be conducted to ensure the appropriateness and effective usage of the policy. These reviews may result in modification, addition or deletion of the policy to better suit the institution's information needs.
- The ICTS department will always be in a position to assist members in understanding this policy.

14 Consequences of Violation

- Violations of the ICT policy will be documented and can lead to revocation of system privileges and or disciplinary action.
- Before utilizing the institution's ICT resources users are expected to sign an acknowledgement of the ICT policy and a copy of acknowledgement will be kept of the ICTS office.

ACKNOWLEDGEMENT

I have read the ICT policy. I understand the contents and I agree to comply with the said policy.

Location…….....
Name……..
Employee's Signature……. Date……..
Supervisor Signature……Date ……

Revision Dates

Date Revised	Reason	Authorised By	Signature