LUPANE STATE UNIVERSITY

ICT Policy

www.lsu.ac.zw

P O Box AC 255, ASCOT, BULAWAYO
ZIMBABWE

Date effected: ……/……/……

Date last updated: ……/……/……...

Table of Contents

1.0 Preamble

The Information and Communication Technology Services (ICTS) Department is the hub that supports the day to day ICT related operations of the institution. The Department seeks to establish policy, standards, guidelines and procedures to ensure that ICT facilities, services, programs and data are protected from all threats, whether internal or external, deliberate or accidental .The ICTS Department will endeavor to ensure that these technologies are used in a responsible manner through crafting of policies which guide users. This ICT Policy document seeks to provide guiding principles that ensure compliance, acceptable and secure use of ICTs by the LSU community. The University acknowledges the convergence of technologies such as the Internet and mobile technologies which provide a valuable resource for teaching and learning. This policy also seeks to ensure that the telephone system is used appropriately and that call charges are kept to a minimum.This document reflects the general policy guidelines and strategies that the University is prepared to pursue with regard to ICTs and some of the regulations that would facilitate their successful implementation in the University. This ICT policy therefore seeks to provide guidelines for acceptable use, compliance and a secure use of ICT's by the University community.

1.2 Definition of terms

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

1.2.2 Where the terms "ICTS Department", "ICTS" or "Department" are used, they will refer to the Information Communication Technology and Services Department of the University.

1.2.3 The term "ICT" refers to any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes all digital and electronic information storage, software and communication media devices such as, telephone, mobile phones, faxes, PABX systems, wireless or computer networks, workstations including laptops, personal digital assistants (PDA), electronic e-mail systems and the Internet.

1.2.4 The term "user" refers University staff members, students and any authorised person who accesses an ICT system, service or equipment owned, managed or supplied by LSU.

1.2.5 "E-learning" means all forms of interactive instruction which is enhanced, supported, mediated, delivered or accessed by electronic means.

1.2.6 "E-content" in this policy document is used as a short form of 'E-Learning content'.

1.2.7 "CMS" means Content Management System such as Moodle, which allow development, management and integration of learning material.

1.2.8 M-learning is defined as learning that happens when the learner takes advantage of the learning opportunities offered by mobile technologies where there is no fixed learning venue/environment.

1.2.9 "BYOD" means Bring Your Own Device and is a concept where users are allowed to use their personal mobile devices to access University data and systems.

1.2.10 Appropriate and responsible manner means use that is consistent with the mission and vision of the University allowing LSU to achieve its objectives.

1.2.11 Restricted or objectionable material refers to any material that may be sent over the Internet that by its nature could result in drug misuse or addiction, hate speech, crime, incitement, pornography and any other material which contravenes the Laws of Zimbabwe or other international conventions which the country is signatory to.

1.2.12 Copyrighted content means material for which the copyright for the content is held by a third party other than the University examples include music, computer software, films, video and Academic Intellectual Property.

1.2.13 Hardware is a collection of physical parts of a computer and associated peripherals e.g. monitor, keyboard, laptop, switch, router and many others.

1.2.14 Internet is used to refer to a global network of computers providing a variety of information and communication facilities.

1.2.15 VPN is a network technology that creates a private secure network connection over a public network such as the Internet.

1.2.16 DHCP refers to network protocol that enables a server to automatically assign an IP address to a computer from a defined range of addresses configured for that network.

1.2.17 PDA is a palmtop computer that functions as a personal organiser and also provides email and Internet access.

1.2.18 ATM is an unintended electronic machine erected in a public place, which allows customers to complete basic transactions after being authenticated through a personal Identification number.

1.3 Objectives

1.3.1 To improve and promote efficient use of information systems, and enhancing information security systems at LSU.

1.3.2 To provide a framework for the establishment, expansion and management of ICT, a secure network that provides enhanced ICT services at a manageable cost;

1.3.3 Provide a framework that define procedures for developing Software projects in the University;

1.3.4 Maintenance of confidentiality and integrity of information held by the University.

1.3.5 To support proper acquisition and disposal of ICT equipment.

1.3.6 To prevent bad publicity or putting the name of the University into disrepute.

1.4 Scope

The policy lays out plans and procedures that ensure the protection of the confidentiality, integrity and availability of the ICT resources granted to staff, students and visitors of the University. The ICT policy document relates to all Information and Communication Technology facilities and services provided by LSU's ICTS Department including, but not limited to computing devices, e-mail system, databases, integrated systems, operating systems, eLearning systems, Internet, telephone systems, wireless communication, printers and photocopiers. All LSU employees, volunteers, students, associates and partners are expected to adhere to it.

1.5 Responsibilities

1.5.1 The University Council is ultimately responsible for the existence and monitoring of the implementation of the ICT policy.

1.5.2 The Vice-Chancellor is responsible for the effective implementation of this policy in terms of necessary processes and procedures at the institutional level.

1.5.3 The Computer Committee has the responsibility for the review and recommending approval of the University ICT Policy and any other ICT related policies.

1.5.4 The Director, ICTS has the responsibility to oversee the overall management and operation of the University's ICT infrastructure and services, consistent with the strategic and operational objectives of the University, and for information security, its governance framework and ensuring that the ICTS Department implements the agreed policies.

1.5.5 The user's primary responsibility is to adhere to the University's ICT-related policies.

2.0 General Acceptable Use

All users must comply with the following:

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

2.1.2 Do not attempt to gain unauthorised access to information or facilities. It is an offence to obtain unauthorised access to any computer or to modify its contents. If you do not have access to information resources you feel you need, contact the ICTS Department for assistance.

2.1.3 Disclosure of personal system passwords or other security details to other staff members is not allowed. If someone else gets to know your password, ensure you change it or get ICTS support to help you.

2.1.4 ALWAYS check external removable disks (flash drive, memory cards and external disks) for viruses, even if you think they are clean.

2.1.5 Do not access, publish, bookmark or download obscene or pornographic material using the University's facilities.

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

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

2.2 Non-compliance

2.2.1 The University's ICT resources exist and are maintained to help the organisation reach its vision and mission. The University reserves the right to monitor the use of its ICT resources

and to deal appropriately with users who use its ICT resources in ways that are contrary to the conditions of use set out in this policy.

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

2.3 Password Policy

2.3.1 All system-level passwords such as root, enable, Windows server administration, application administration accounts, shall be changed after four (4) months.

2.3.2 All user-level passwords such as e-mail, web, and desktop computer shall be changed at least once every six (6) months. Administrator passwords shall be changed every four (4) months.

2.3.3 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" shall have passwords distinct from all other accounts held by such users.

2.3.4 Passwords for the University accounts shall not be used for other non-University access such as personal ISP account, Yahoo Mail, and Bank ATM.

2.3.5 All passwords shall be treated as sensitive and confidential University information. Users shall not share the University passwords with anyone.

2.3.6 Users shall not use the "Remember Password" feature of applications like Outlook, and Firefox.

2.3.7 Users shall not write passwords down and store them anywhere in their offices.

2.3.8 New ICTS members of staff and students on attachment to the Department shall be assigned Administrator passwords for effective administration and monitoring of computer applications.

2.3.9 On termination of contract for staff members and students on attachment, passwords will be immediately changed.

2.3.10 The user's password shall be alphanumeric, contain a minimum of 8 characters and a maximum of 14 characters and no dictionary words are to be used.

2.3.11 Passwords cannot contain the user name or parts of the user's full name, such as his first name.

3.0 University Network

3.1.1 The ICTS Department will plan, deploy and support a campus-wide ICT network as a basic infrastructure service for the facilitation of sharing electronic information and resources by University staff and students as well as partners engaged in legitimate University business as may be determined from time to time. Activities that interfere with the reliable operation of the Network are prohibited which include, but are not limited to: operating network-capable devices that attack the Network, cordless phones and other devices using unlicensed radio communications spectrum; and impersonating or interfering with Network equipment or Network services. The Network is a critical University resource therefore:

3.1.2 The University Network will be designed and implemented so that it enables interconnection between sites to allow for enterprise data to be exchanged via Mopane the University MIS, Koha and Pastel.

3.1.3 Through provision of wired and wireless networks, staff and students must enjoy seamless connectivity to facilitate research, teaching or general administrative work.

3.1.4 The campus Networks will connect into a VLAN providing the backbone.

3.1.5 All network expansion and design must take account of new emerging technologies and standards.

3.1.6 Only authorised staff members from ICTS Department shall install and maintain active network equipment that connects to the backbone Network.

3.1.7 All computing devices that are connected to the University Network shall have an up-to-date antivirus software installed to prevent viruses and all other forms of malicious code.

3.1.8 All servers shall be installed with an antivirus and only authorised personnel allowed to login. An audit trail must be kept to track changes made.

3.1.9 The locations and IP addresses of all hubs, switches, routers, and firewalls on the network must be documented.

3.1.10 The range of all IP addresses assigned by all DHCP servers on all subnets must be documented.

3.1.11 Configuration information about how the server is configured including, event log settings, security settings and a list of services running shall be documented.

3.1.12 Document Administrators on the server with a list of rights of each Administrator.

3.1.13 The authentication process and protocols used for authenticating Administrators and users on the server must be documented.

3.1.14 Intrusion detection and prevention method used on the server on the server should be documented.

4.0 Network equipment security

4.1.1 All communications cabinets and rooms shall be locked at all times.

4.1.2 Access to any ICT Network equipment shall be restricted to designated members of staff of the ICTS Department.

4.1.3 The ICTS Department will maintain up to date Network diagrams that define the Network topology and IP addresses and core Network equipment configuration.

4.1.4 Only authorised ICTS personnel will have their biometric fingerprint captured for accessing the server room.

4.1.5 Access rights to the network will be allocated based on the user's role.

4.1.6 Users are responsible for ensuring their password is kept secret.

5.0 Internet and E-mail

This section governs the use of the University's Internet and electronic mail (e-mail) system to facilitate the exchange of electronic information both internally and externally to create a safe and secure environment for staff and students and other users when undertaking University business and research over the Internet. 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 leads to degradation of network performance, or in extreme circumstances could take the whole of the University network down or lead to loss of vital information resources. Using the University's Internet infrastructure 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 the Laws of Zimbabwe or other international treaties.

5.1 General

The University will normally provide an e-mail account to all staff and students, based on their duties or activities at the University. The University may also provide an e-mail account for alumni, students on attachment, and visiting lecturers, as well as others. All e-mail accounts and associated addresses are the property of the University. The centrally administered e-mail account will be considered the individual's official University e-mail address. It is the responsibility of the account holder to ensure that e-mail received at his/her official University address is attended to in a timely manner.

5.2 Creation and deactivation of accounts

5.2.1 Activation

Staff accounts are created when the Human Resources section has notified the ICTS Department on new employees that have joined the University and whose job demands the use of email. Each User will have two email accounts created, from the University domain (abc@lsu.ac.zw) and from Gmail (abc@lsu.ac.zw) which will be centrally administered.

5.2.2 Deactivation

When an employee is terminated in the Human Resources system, that employee's email account will be deactivated. The mailbox will not be immediately deleted since it is a University resource. Special arrangements are made in cases where the employee's account was used for receiving external email related to University business.

5.3 Use of private e-mails

Use of private e-mail for University business is not allowed as LSU's business information will be stored in private inboxes, should an employee resign it will be difficult to follow up on their private e-mail. When private e-mail accounts are used University information is at risk in terms of security and privacy. When the University e-mail system is temporarily down, staff will be asked to use the LSU registered Gmail accounts. The e-mail lists generated for formal University

communications must not be used for transmitting any messages such as chain letters, buying and selling or any other use other than University business.

5.4 Computer Viruses

Incoming and outgoing e-mails and their attachments may carry dangerous or potentially 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.

5.5 The user will:

5.5.1 Be responsible for all electronic mail originating from the User's ID;

5.5.2 Not forge, or attempt to forge, electronic mail messages or signatures;

5.5.3 Not attempt to read, delete, copy or modify the electronic mail directed to other users without prior consent;

5.5.4 Not send, or attempt to send, harassing, derogatory, obscene and/or other threatening material to a user of any e-mail service;

5.5.5 Not send 'for-profit' messages or chain letters,

5.5.6 Not subscribe to newsletters, health programs, social media alerts or any other social activity using University mail.

5.5.7 Not use the Internet in any way that involves accessing entertainment or gambling websites or other websites which have no legitimate connection to the University's business;

5.5.8 Will have a maximum inbox size of 1 GB and will be responsible for maintaining the inbox.

5.5.9 Keep logon passwords confidential;

5.5.10 Report any security lapses/concerns to the ICTS Department

5.6 Confidentiality

E-mail communication is not always a secure means of communication across the Internet.

5.6.1 The Internet is a public domain and all users must be cautious when sending strictly confidential or commercially sensitive messages because privacy cannot be guaranteed.

5.6.2 Employees shall have no expectation of total privacy in anything they store, send, or receive on the institution's e-mail.

5.6.3 ICTS Department shall endeavor to uphold the individual user's privacy and confidentiality of their e-mails but may access the individual's inboxes in case of sickness or at the request of the head of department to track business communication.

5.6.4 During system administration authorised ICTS personnel may have access to e-mail accounts and their contents. ICTS staff may monitor e-mail usage to ensure server and protocol availability, get mail server statistics, perform message count, trace blocked spam messages and facilitate proper sending and receiving of messages.

5.6.5 The ICTS Department may take special actions in administering e-mail such as deleting e-mails if this is essential to preserve the integrity of the system.

5.7 Writing business E-mails

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

5.8 ICTS Department E-mails

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. The Department 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. Where the ICTS Department becomes aware that there might be downtime during working hours as a result of network failure e.g. ISP network problems, these will be communicated on time. It is crucial to read e-mails from the ICTS Department as they convey important announcements and notifications.

6.0 Software development, support and use

The Department will endeavor to develop software in-house or use open source software to reduce expenditure on licensing where possible. The Software Development Section shall provide systems development and support for University wide applications. However Departments and Faculties may be allowed to buy software or customise software limited to internal usage. The Departments and Faculties planning to buy software will need to acquire pre-approval for purchase from ICTS.

6.1 The principles that underpin the purchase of software shall be:

6.1.1 Sound academic or administrative rationale

6.1.2 Compatibility with University systems and durability of the required software.

6.1.3 Value for money

6.2 Objectives

6.1.4 The purpose of this section of the policy is to ensure that the process of software development in the ICTS Department follows the due process right from the planning phase through to the implementation stage and that all deliverables at every milestone meet the required standards.

6.1.5 This policy also seeks to continually improve on the process of software development in the ICTS Department, ensure that the software products produced meet the requirements of the user and are of good quality.

6.1.6 This policy also addresses the need for software support and use of the available information to ensure that the integrity of the system is not compromised at any time.

6.3 Scope

The policy covers the development and support guidelines within the University. The policy also covers the support required for any operational Information Systems, integrity of data, request for service, and accessibility of information.

6.4 Policy statements

The Software Development Section within ICTS Department shall be responsible for developing, and maintaining University wide administrative and academic systems.

In-house software development life cycle shall involve the following steps:

6.4.1 Project inception

For any software development work to commence, a requesting Department/Section shall submit automation requirements or a change request form which should be signed by the requesting Department/Section head to the ICTS Director.

6.4.2 Planning and analysis

After the request has been approved, the Software Development Section shall carry out a feasibility study of the request. If the project is deemed feasible, a project plan shall be drawn, stating the duration and scope and a requirements analysis document shall be drafted by the Software Development Section and signed by the requesting Section and approved by the Director, ICTS.

6.4.3 Design

Using the requirements analysis document, the Software Engineer shall design the system. The main design documents required are the Process Flow Diagrams, Use Case Diagrams, Data Flow Diagrams and Entity Relationship Diagrams.

6.4.4 Development

At this stage the actual logic of the design shall be implemented through code by programmers. Any changes to be made to the database shall be approved by the ICTS Director.

6.4.5 Testing and implementation

Once development is complete, unit tests and integration tests shall be carried internally. Afterwards, the system is tested with the end users through user acceptance test with reference to the specified requirements. If all user requirements have been met, the project shall be signed off.

6.4.6 Maintenance and support

The User Support Section shall be trained on all implemented features of the system. The Section shall, in turn, train the end users.

6.4.7 **Monitoring and evaluation**

The Software Engineer shall put in place modalities for ensuring that the systems developed are reviewed annually or such a time deemed fit to find out if the system is still fulfilling the user requirements, and if not, appropriate actions taken to ensure that the system meets the ever-changing user needs. A system that is too costly to maintain, does not meet user requirements or is deemed to be obsolete shall be retired after consultation with all stakeholders.

6.5 Data backup and restoration

All ICTS sections that operate key University systems including Software Development shall formulate and implement systematic schedules for performing regular backups on the systems in their custody.

The ICTS Technical Manager shall be responsible for ensuring that backup procedures are followed. Back up data shall be stored at an external location from the institutional data repositories.

6.6 User Support services

The ICTS Department acquires and develops a variety of ICT technologies, products and services in response to the academic business and related requirements of the University. Upon production, these requirements are distributed (or made available) to users. Thereafter, continuous and tailored support is necessary in order for the users to fully exploit them. A policy guideline is necessary for this support.

6.7 Support coverage

6.7.1 Support sites shall be designated by campus sites.

6.7.2 User Support Technician(s) will be posted at each campus.

6.7.3 ICT Support personnel shall be deployed in accordance with the assessed support load per support site (or campus). The load shall be proportional to the extent to which ICTs are in use, determined mainly by the expansion of the University network and number of users there off.

6.8 Procurement Support

The ICTS User Support Section shall assist users in deriving the technical requirements and specifications of all ICT acquisitions and purchases. The User Support section shall verify all ICT acquisitions and purchases for approval by the ICTS Director. All purchases should be in line with the University procurement policy.

6.9 Infrastructure Support

The ICTS Technical Manager shall assist users in carrying out design, requirements specifications, and preparation of Bill of Quantities, material acquisition and supervision of implementation of all ICT infrastructure at the University.

6.10 Hardware Support

6.10.1 The User shall be responsible for the basic daily care of ICT hardware under their care.

6.10.2 The User Support section shall support hardware that is found in offices, computer rooms, laboratories and lecture theatres. Such hardware may include servers, desktop computers, laptop computers, printers, scanners, digital cameras, liquid crystal display (LCD) projectors, PDAs (palm or pocket PC), UPSs, network access hardware, among others.

6.10.3 Only authorised University ICT Technicians will be allowed to repair faulty equipment. During the warranty period, no attempt should be made to repair faulty hardware but should be sent for repairs to the supplier in its original packaging.

6.10.4 Where necessary the User Support section shall escalate user support requests to appropriate ICTS Sections and to other University sections.

6.10.5 Every campus shall have a stock of support tools consisting of items as determined by the support work within. In addition, a stock of shared tools shall be maintained centrally at main ICTS Office.

6.10.6 Support personnel shall be supplied with protective and safety clothing and gear suitable for the tasks involved in the support activities. These shall include items such as work suits, dustcoats, dust masks, safety gloves and other items as the management of ICTS Department may determine from time to time.

6.10.7 Towards realising the set support standards such as turn-around time and low down time, the ICTS Department shall ensure availability of logistical resources for transport to ensure

rapid movement between support sites and communications to ensure contact between support personnel.

6.10.8 A schedule for preventive maintenance shall be drawn, recognising every piece of hardware. Preventive maintenance shall be carried out according to the recommendations of the manufacturer of the hardware, in terms of frequency and method of maintenance. However, where justified by the case, service shall be provided on the basis of request.

6.10.9 Equipment bought on Service Agreements shall as far as possible be placed on maintenance contracts.

7.0 Safeguarding access to workstations

Workstations should not be left unattended as this provides an opportunity for intruders to access documents and the e-mail system and send items in another user'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.

8.0 Equipment movement or 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 University. Security is authorised to stop and question any person leaving University premises with ICT equipment or software. An application for removal of University equipment from premises must be filled and signed by the Security Officer, Asset Section – Bursar's Department and ICTS Director or the Technical Manager before ICT equipment is taken out. The form must be filled in triplicate.

9.0 Hardware acquisitions

All computers and associated accessories will be sourced from a reputable supplier(s) in liaison with University's Buying Section. All computers and associated devices such printers, scanners, routers etc. used on the University network, should be registered in the University ICT's inventory. Acquisitions shall be guided by the following steps:

9.1.1 A memo from the relevant Department requesting new hardware must be signed by the requesting Head of Department.

9.1.2 The ICTS Department then evaluates if there is a need for the purchase of new hardware as per request.

9.1.3 Three quotations are requested from registered suppliers and a Purchase Voucher is processed and sent to Bursar's Department for processing.

9.1.4 Upon approval by Bursar's Department, the supplier is contacted to supply requested ICT equipment.

9.1.5 On delivery all new hardware or software is assessed and tested to ensure compliance to specifications. Once the equipment is compliant, a Goods Received Voucher processed and is submitted to the Bursar's Department so that the payment is processed.

9.1.6 The general life span of hardware should be determined. This is useful for auditing purposes and valuation of computer equipment. Scheduled replacement may also be possible after the lifespan has been determined. The following are guidelines for hardware life spans:

- Desktop : 5 years
- Laptop : 3 years
- Servers : 3 years

10.0 Disposal of ICT Equipment

ICT hardware shall be declared obsolete according to the recommendations of the manufacturer and the relevant University policy and regulations e.g. Depreciation of Assets Policy. The User Support section shall periodically conduct maintenance to identify, retire and replace the hardware categorised as at "end-of-life."

10.1 Disposal or reallocation of equipment

All ICT equipment no longer required within the service for which it was purchased should be reported to the ICTS Department. The Department will examine the equipment and determine the best course of action. The equipment will either be reused, at which time any data remaining on the device will be digitally shredded or will be securely disposed of.

10.1.1 **Procedure:**

The ICTS Department, through constant monitoring of its inventory, ascertains which equipment is due for replacement and disposal. All other university departments will also communicate with the ICTS department.

ICT equipment may be disposed of in the following ways:

(i) Recoveries from offices/ computer laboratories – During the constant service and maintenance rounds the ICTS personnel may extract all gadgets that they deem obsolete from any office or laboratory and replace the equipment accordingly.

(ii) Hardware sale - Obsolete hardware may be sold at salvage value. The Bursar's office may assess the hardware and advise appropriate market price for the hardware sale. The Bursars department may also advise on the procedures of hardware sales. All hardware for sale should be presented to the ICTS User Support Section for technical inspection to ensure that it does not have any licensed software or university information and replace with free versions before disposal.

(iii) Hardware donations of obsolete hardware to community outside the university should follow guidelines laid down by national policies on deployment of used technology equipment and environmental conservation. Hardware can be sold or donated to deserving communities, recyclers that include collectors, importers and assemblers.

(iv) Hardware destruction - Obsolete hardware that may neither be salvaged, nor sold nor donated may be destroyed. An inventory of hardware that has been destroyed or is due for destruction must be maintained. All hardware destruction should be done in accordance with available hardware destruction statutes or legal requirements.

10.2 Disposal of removable media

All items of removable media which are no longer required should be disposed of with regard to the data stored on the device. Physical destruction of the media is the most secure method of disposal and this should be carried out on all CD/DVDs.

10.3. Disposal of printed material

Care should also be taken when disposing of printed output. If sensitive data is contained within the document, the document should be disposed of in confidential waste and/or shredded.

10.4. Disposal of cartridges and tonners

All used cartridges and toners will be collected from offices will be handed to the Bursar's Department for sale to companies in the business of recycling cartridges. If there are no buyers the cartridges will be disposed.

11.0 Training

11.1 Training of ICTS staff

The Department shall periodically expose ICTS staff members to refresher courses and workshops so that the Department is abreast with ever changing technology.

11.2 Training of Users

It is desirable that all University staff be literate users of ICT services, the level of literacy being in line with the demands of their job functions. Training shall be conducted on a continuous basis focusing on building skills in users making them effective in exploiting ICT resources, products and services.

12.0 Computer laboratories and ICT hardware usage

12.1.1 Rooms containing ICT hardware such as Computer Laboratories may only be entered if an ICTS staff member is present.

12.1.2 Bags must remain outside the computer laboratories.

12.1.3 Food and/or drinks are not to be brought into computer laboratories.

12.1.4 Computer equipment must not be swapped around (e.g. changing of keyboards, mice from one computer to another).

12.1.5 Students must not attempt to access the inner working of a computer or ICT device outside of its normal use.

12.1.6 All equipment faults and/or damage must be reported to the ICTS personnel immediately.

12.1.7 All ICT gadgets in the computer laboratories, including Local Area Network equipment, Internet and e-mail are to be used for teaching, learning and research purposes only.

12.1.8 Playing of software games or downloading inappropriate content is prohibited.

12.1.9 Students must adhere to the laws concerning piracy, copyright and other Intellectual property rights.

12.1.10 It is illegal to retrieve, view, post, store, or distribute pornographic, obscene, violent or offensive material through the University's e-mail, network or hardware infrastructure.

13.0 Funding for ICT related acquisitions and services

The University shall set aside a certain levy on students' fees for continual development and improvement of the University's ICT infrastructure.

14.0 Laptops and Mobile devices

This section of the ICT policy relates to the use of laptops or any other mobile devices provided by the University to staff members for work and other tasks including, but not limited to administrative, research and lecture delivery. All LSU employees, volunteers, students and associates are expected to adhere to it.

14.1 The user shall:

14.1.1 Be responsible for the security of the laptop or the mobile device at all times;

14.1.2 Not install unauthorised software or material.

14.1.3 Not attempt to read, delete, copy or modify the system files of the device.

14.1.4 Report loss or theft of the device to the ICTS staff or management immediately.

14.1.5 Will be required to replace the lost or stolen device otherwise provide information to the Insurer who will determine if the loss is not due to negligence of the user. The Insurer may cover replacement costs depending on circumstances surrounding loss or damage of the device.

14.1.6 Locking the device in a secure location when it is not in use.

14.1.7 Changing the password as often as required by the University ICT policies.

14.1.8 Ensuring that the ICTS Department has provided a functional Anti-virus, Firewall, or Encryption software.

14.1.9 Return the device(s) provided by the University in the event of termination of employment.

14.2 **Abuse of Laptops and mobile devices**

If there is any reason to suspect that the laptop or mobile device is being used for any purpose that contravenes the University's policies, the ICTS Department reserves the right to inspect the laptop or to take any measure that may be deemed necessary.

14.3 **Confidentiality**

Employees shall have no expectation of privacy in anything they store, send, or receive on the institution's laptop or mobile device.

14.4 **Disposal**

At the end of life of the mobile device, the user shall bring the laptop or mobile device to ICTS Deaprtment for backup of old data and issue of new device where applicable. ICTS shall format the device to delete all University data in it. The Bursars' Assets Section will determine method of disposal of the University asset.

15.0 Bring your own Device (BYOD)

15.1 Purpose

The current socio-economic environment may not allow the institution to provide a computing device for every staff member and student. To enhance teaching and learning, staff and students may use their own device and will be given login credentials to access our electronic resources. With lecturers' approval, students can access the Internet in the classroom to collaborate with other students. This section of the policy shall be used in conjunction with other supporting sections of this policy and other related policies of the University. Violations to the University ICT policy may result in disciplinary action, revocation of privileges even when the violations are committed using one's own device.

15.2 Connectivity

The ICTS Department shall support all connectivity issues and all users shall contact the Department for connectivity related support.

15.3 Reimbursement

The University shall not be liable to reimburse users that connect to the University network for work or research with their own device should the device get damaged presumably during its connection to the University network or systems.

15.4 Security

15.4.1 Physical security of personal devices connecting to the University network shall lie with the owner. Where such devices get lost a report shall be made to the Security Department.

15.4.2 The owner shall be responsible for the download of security patches of their operating systems as well as updates of their own Anti-virus programs. Where any challenges are faced the user may approach the ICTS Department for assistance.

15.4.3 Users shall not download sensitive University data found on any of its systems into personal devices unless otherwise approved by their supervisor, where such data is to be used off campus it has to be encrypted all the time.

15.4.4 Users must read and understand security issues covered under Internet and e-mail sections of the policy as it is applicable when one is using their own device.

15.5 Hardware maintenance of privately owned devices

The ICTS Department shall not take responsibility for the maintenance, replacement, repair or upgrade of privately owned equipment and accessories.

16.0 Telephone Usage

16.1 Purpose

To provide guidance on the use of telephones, the conditions for personal use and general guidelines on the use of telephones. The section also stipulates what criteria is used for providing telephone services to staff members. LSU is keen to ensure that telephone services are provided to all members of staff to ensure smooth and efficient communication externally and internally. This section lays down procedures for using the telephone, making and receiving business and private phone calls. All staff members should be made aware of the standards expected of them when using the phone and of any additional Departmental arrangements.

16.2 Policy Statements

16.2.1 The telephone system is an organisational resource whose use may be monitored. A call logging system which records details of every call made both internally and externally shall be installed in all the University's campuses.

16.2.2 Telephone handsets shall be provided to enable staff members to perform their duties in conducting University business.

16.2.3 Where there is a need to call mobile and trunk calls, members shall be allowed to make these calls but they must be approved by the Departmental / Section heads.

16.2.4 Principal Officers, their Deputies, Deans and Directors shall be allowed to call mobile phones and trunk calls while Chairpersons of the department shall be allowed to make trunk calls.

16.2.5 Local calls made from desk landline phones are totally at the discretion of the staff member and it is the responsibility of each staff member to ensure that calls are appropriate to their work and are conducted expeditiously.

16.2.6 Where telephone extensions are barred from making local calls or any other calls, calls are to be placed through the Switchboard Operator, whose duration may be recorded.

16.2.7 The University acknowledges that, from time to time, staff members may need to contact their family while they are at work. It is expected that these calls shall be brief, infrequent and not tie up University lines. The University shall monitor call volumes and any staff members who abuse this facility will be asked to pay for the call charges.

16.2.8 Where employees make business calls on their personal mobile phones they may submit an expense claim for the cost of those calls provided that the calls were approved by their Head of Section/Department.

16.2.9 Calls shall be answered promptly. The receiver must clearly state their name and department.

16.3 ELearning

The purpose of eLearning is focused at consolidating some of the strategic directions that LSU wants to pursue related to teaching and learning. The University will ensure that its eLearning provision can

meet the needs of a full range of flexible and independent learning experiences. This will include on and off campus learning, which will cover blended and full eLearning courses.

16.4 Objectives of eLearning

The objectives of the policy section covering eLearning are:

16.4.1 To provide an alternative education delivery system for greater access by our students;

16.4.2 To provide flexibility of time and location;

16.4.3 To promote the integration of technology in the learning environment;

16.4.4 Continually increase usage of on-line learning resources for new students, induction and continuous performance improvement.

16.5 Policy Components

This section of the policy shall guide LSU's eLearning initiatives and programs. This policy has the following components.

16.5.1 **Quality Assurance**:

16.5.1.1 E-content development shall adhere to the University's learning and teaching quality assurance processes and meet all required standards.

16.5.1.2 The University shall establish an appropriate e-content quality assurance process.

16.5.1.3 Successful E-content presentation structure shall be standardised and pass a Departmental peer review process.

16.5.2 **Intellectual Property Rights and Ownership:**

E-content whose development is initiated and fully supported by the University belongs to the University.

16.5.3 **Capacity Building for eLearning:**

16.5.3.1 All staff involved in development, management or use of e-content shall be provided with continuous and appropriate training.

16.5.3.2 Regular refresher courses shall be provided to staff and will be based on needs.

16.5.4 Management and support of eLearning

The ICTS Department shall be responsible for the creating, publishing, customization and management of eLearning systems by liaising with assist academics in the creation of content. The Department will also be responsible for publishing completed e-content on behalf of the University and the maintenance of eLearning servers.

16.5.5 **Security and Access Rights**

Access to e-content that belongs to the University will be restricted to bona fide University staff, students and other authorised people.

16.5.6 **Student eLearning accounts**

The student will use their accounts for accessing eLearning resources via the student portal. Students will be responsible for maintaining their accounts.

16.5.7 **Access to eLearning Content**

The ICTS Department shall be responsible for providing and maintaining appropriate and sufficient infrastructure that supports access to eLearning resources.

17.0 Web Policy

The University's web presence is a key communications medium to promote and enhance the University's image by providing relevant and up-to-date information about University programs, research, services, and accomplishments.

17.1 Scope

This policy governs the use of the University website, www.lsu.ac.zw. The University's website is distinctive for its integrated user experience, widely distributed publishing responsibility and flexibility to allow customised content. With such distributed publishing responsibility comes shared responsibility for quality assurance, usability, performance and security. The actions of one individual or department can affect the entire system. Therefore, expectations are set to ensure quality, manage risk, and present the university's web content to users in the most effective ways.

17.2 Policy Statement

The purpose of this policy is to establish basic requirements for use of university web resources in a manner that maintains quality and appropriately reduces risk to the confidentiality, integrity and availability of university data, as well as the system. The requirements of this policy deal with university standards for web content, including visual identity, design and editorial quality, accessibility, management applications and databases, security and advertising.

17.3 Definitions

Software application used to store, edit and publish Web pages, including html, text, photos, video, and other media via a series of managed templates.

Domain: A domain name locates an organization or an entity on the Internet. In case of Lupane State University our domain name is www.lsu.ac.zw. Web sites that use a name that includes lsu.ac.zw are considered part of the domain.

University Web site: Web sites that represent administrative departments and academic units of the university. These Web sites are university assets and should follow university policies and procedures.

University Web Content: Any content or data created by university faculty and staff and published on the university Web site to represent the work of the university, faculty, department or unit. Web content is primarily hosted by the university on the domain www.lsu.ac.zw. In addition, some university Web content is externally hosted by outside firms. Such hosting relationships are managed and guided by university contracts.

LSU considers online publishing to be an essential resource for communication, research, marketing, and administration thus proper utilization of the website and other online resources is vital. The University still reserves its right to define and limit the terms of use of its online systems. Appropriate university resources may be used to create and publish web pages, the purpose and outcome of the published information being in full support of LSU's vision and mission. This entails that LSU web content must relate to the official activities and functions of the University.

17.5 Policy

All university web content presented on the Internet will be governed by this policy. Web content will be supported on the domain www.lsu.ac.zw. Faculty, staff and students using university resources to develop and present university web content will abide by standards designed to assure quality, performance, usability and security. An integrated user experience is assured through the use of a content management system and a series of design templates that provide reasonable publishing flexibility. Editorial and design standards ensure consistency of the experience for users across the site. Standards for timeliness and accuracy assure quality as well. Content publishers will be provided training and on-going support to effectively use these tools and standards.

Performance and security standards assure that the site functions properly and the university's data, including personal student data, is protected, as well as the university's reputation and good name. Performance problems, security risks or poorly presented content on one part of the site can affect the entire domain.

Special Web applications and databases presented on the site will adhere to university standards referenced in this policy. Applications that rely on university data, including confidential, official use only and unrestricted will follow appropriate requirements.

Applications that pose security risk, hinder performance or confuse the user will not be hosted on the site or have a link on the website.

External hosted university Web content should be explicitly reviewed and approved by the ICTS department, following review of unique requirements that would warrant such hosting. Content that is linked from the university's Web site to another entity or organization's site should clearly identify a departure from university pages. Non-university Web content should not use or replicate the University's templates in a manner that confuses content ownership.

17.6 Standards

Design standards for university Web pages maintain an integrated user experience and look across the site and as such standards are set by the ICTS department.

Editorial standards for headlines, copy, style and content maintain an integrated user experience and voice across the site.

17.7 Timeliness and Accuracy:

Content owners and content publishers are responsible for maintaining Web content that is accurate and timely. Publishers should ensure proper maintenance, and follow all published university standards of form and content.

18.0 Data privacy

This section of the policy relates to information gathered through various forms by personnel from the ICTS department and spells out how the information is handled.

18.1 Personal information about students and staff for purposes, such as communicating with them, providing access to the student and staff portals and the associated services, processing payments and providing other client services.

18.2 When staff members join the University and students register, information may include information provided via the application form or other forms, such as name, address, e-mail address, and other personal information.

18.3 Staff and students will be informed on how personal data will be used.

18.4 Personal information will be used in an ethical manner.

18.5 Not to disclose sensitive personal data which may include remuneration, health status, criminal records etc.

18.6 The University may share personal information described above with its affiliates for authorised legitimate purposes and as permitted by applicable Laws.

18.7 Although every effort is made to secure network communications, LSU cannot guarantee the privacy of online communications, individuals using online services should also take steps to protect personal information, such as closing the Web browser when finished using the site.

18.8 As data stewards all members of the ICTS Department should sign an acknowledgement to this policy, which will be filed at the Director's Office.

19.0 Access Rights and group policy

Modern applications and systems contain massive amounts of sensitive organisational information. Although immediate access to the information increases employee productivity, it also heightens the risk of data theft and unauthorised data access from a number of sources. The ICTS Department will take steps to ensure the confidentiality and integrity of critical University information. The Windows Authorization Manager will be used which comprise of the following:

19.1.1 A role-based user interface. This interface is used by application administrators to define roles and to specify user access through user or group assignment to roles.

19.1.2 Management programming in interfaces: These interfaces enable administrators to configure access control for roles, assign groups and individuals to roles and view audit logs.

19.1.3 Enforcement functionality: These features enable application to query and enforce policy rules.

19.2 Components of the Authorization Manager

19.2.1 Protects sensitive data and ensures compliance: Authorisation Manager helps protect intellectual property and data by limiting application access to authorised users and groups. It helps ensure compliance with data-related regulations with audited, directory-based access control.

19.2.2 Simple and centralised administration: Authorisation Manager provides a simple, common, role-based administration experience. Administrators need to learn fewer authorisation models and require less training.

19.2.3 Platform integration and alignment: Authorisation Manager provides support for Windows platform features such as Active Directory groups, Windows security auditing and Microsoft Management Console (MMC).

20.0 Social media

University employees can use social networking websites, blogs, Wikis, as they communicate in the online world in their personal capacity but must note the following:

20.1 Internet postings should not include University logo unless permission has been granted.

20.1 Internet postings must not violate the privacy, confidentiality, copyright and other Laws.

20.3 Only authorised University personnel will be allowed to post on the University's official social networking sites.

20.4 Disclosure of confidential and proprietary information relating to the University will result in disciplinary action being taken against the individual.

20.1 Data Security

To ensure secure access to data the University shall:

a) Restrict access to records and files containing confidential information to those who need such information to perform their job duties; and

b) Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

c) Encrypt all transmitted records and files containing University data that will travel across public networks, and encrypt all files containing University data to be transmitted wirelessly.

d) Reasonably monitor systems, for unauthorised use of or access to University data.

e) Encrypt all data stored on laptops or other portable devices.

f) Provide reasonably up-to-date firewall protection, system security agent and operating system security patches, reasonably designed to maintain the integrity of the University data.

g) Provide education and training of employees on the proper use of the computer security system and the importance of data security.

21.0 Policy Maintenance & Review

21.1 Periodic reviews shall be conducted to ensure the appropriateness and relevance of the policy. These reviews may result in modification, addition or deletion of the policy sections to better suit the institution's information needs.

21.2 The ICTS Department will always be in a position to assist members in understanding this policy.

22.0 Consequences of Violation

22.1 Upon violation of this policy, the University reserves the right to withdraw or restrict the User's access to ICT resources. Any such suspected breach will be documented and investigated, and may result in disciplinary action being taken against the offender.

22.2 Before utilising the institution's ICT resources users are expected to sign an acknowledgement of the ICT policy and a copy of the acknowledgement will be kept in the ICTS Director's office.

23.0 Outreach

The ICTS Department shall engage in community outreach work such as providing computer literacy training, helping local communities and schools setting up ICT infrastructure and developing management information systems. The Department will engage in consultancy and fundraising activities.

INTERPRETATION

The interpretation of this LSU ICT policy rests with the office of the Registrar.

24. EFFECTIVE DATE

The policy shall take effect on the date it is signed by the Senate and University Council.

25. REVIEW OF POLICY

This policy shall be reviewed as and when the need arises.

Approved:_____

Chairperson – Computer Committee

Abbreviations

CD/DVD – Compact Disc / Digital Video Disc

UPS – Uninterrupted Power Supply

MIS – Management Information System

IP – Internet Protocol

VLAN – Virtual Local Area Network

ATM – Automated Teller Machine

PDA – Personal Digital Assistant

ISP – Internet Service Provider

DHCP – Dynamic Host Configuration Protocol

LSU Policy Use Only:

Version Number: 1:1	**Committee**	**Signature**	**Date**
Date Received:			
Date Revised:			
Date Revised:			
Recommended By	**Computer Committee**		
Approved By	**VEXCO**		

ACKNOWLEDGEMENT

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

Name……
Department…….
Employee Number …….
Employee's Signature……. Date…….

Policy effective after approval by Senate and University Council.

Council Approval Date……..