NJALA UNIVERSITY

ICT Policy, Procedures and Guidelines

Last Updated – November 2018

1 FOREWARD

The adoption and utilization of Information and Communications Technology (ICT) within Njala University is aligned to the University Strategic Plan. The implementation of ICT requires an overall guiding framework to ensure that it's well-managed, complies with legal and regulatory requirements, creates value, and supports the realization of the University's objectives based on globally accepted best practice, guidelines and principles.

In line with the above, the Njala University ICT Policy provides a structure for all the relevant ICT policies to support the achievement of the ICT Vision. Broadly, the policies here within spell out best practice, define roles and responsibilities of all user groups as well as provide guidance in the delivery, implementation and usage of ICT.

Lastly, I wish to acknowledge the efforts of the Directorate for ICT in the coordination of the development of the ICT policy. We all have an obligation to the University to comply with this Policy. This policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law and organisational policies. We therefore welcome feedback to correct for this and in general constructive criticism to improve the clarity and scope of the document; such feedback should be addressed to the ICT Directorate at: ict@njala.edu.sl

---

Vice-Chancellor
Njala University

2 Table of Contents

3 Purpose and Scope

3.1 Purpose

The purpose of this Policy is to describe and document the ICT policies and procedures that will support Njala University goals and objectives within all the teaching, learning, research and administrative units. This geared towards increasing effectiveness and efficiency in all University functions. As such, the development of these policies took into consideration alignment to other existing University functional policies as well as globally recognized ICT practices. The University will accordingly ensure the university-wide dissemination of this Policy to user group categories.

The Policies will be reviewed periodically to ensure they remain relevant and aligned to the goals of the University.

3.2 Scope

The ICT policy applies to all Njala University Schools, Departments, and Units and covers these areas:

1. ICT Governance
2. University Data Communications
3. Cyber Security
4. Software Development and Acquisition
5. ICT Service Management
6. ICT Skills Capacity Building
7. ICT Services Support
8. Telecommunications and Unified Communications
9. ICT Procurement
10. Social Media
11. Software Licensing and Ownership
12. Information Systems and Data Warehousing
13. Special Needs ICT Usage

4 ICT Policy Statement

In compliance with the National ICT policy, Njala University has set out the following policy statement regarding ICT:

i. The University shall ensure sustainable management of the university's ICT and resources through the creation of appropriate policy, advisory management and operational ICT Directorate that will cater for the broad interests of all users.
ii. The University shall assure availability of ICT services in the university through reliable network infrastructure and sustaining emerging new applications.
iii. The University shall assure availability of User-level Data Communication Services, including, centralised document management, Email, Internet /Intranet Services and to promote office computing in all offices.
iv. The University shall enhance and streamline student education, related administrative and managerial processes and improve academic reporting facilities through the implementation of an integrated Academic Records Information System.
v. The University shall improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated online Library Information System.
vi. The University shall enhance and streamline financial management processes and reporting facilities at both central and faculty levels through the implementation of an integrated Financial Information System.
vii. The University shall enhance and streamline the human resource management and administrative processes through the implementation of a Human Resource Information System.
viii. The University shall ensure and require that all students, academic staff, administrative and support staff, and managerial staff are trained on a continuing basis to equip them with the requisite skills to fully exploit the ICT environment in their different functions
ix. The University shall provide for the growth and financial sustainability of its ICT resources through appropriate funding and operational mechanisms
x. The University shall leverage faculty/unit effectiveness and enable easier access to and coverage of university education by using ICT in instruction, learning and research through the university-wide implementation of E-learning.
xi. The ICT Director is responsible for maintaining the policy and providing support and advice on the University's strategy for sustainable development.

5 ICT Governance and Service Management

ICT services in the University shall be managed by the:

1. ICT Directorate
2. Planning and Quality Assurance Directorate of the University.
3. ICT Management Committee and the Systems Automation Task Force.

5.1 The ICT Directorate (ICTD)

The ICT Directorate (ICTD) is mandated to provide leadership in the development, management and use of ICT in the University as follows:

1. Development and implementation of ICT Policies, Strategies and Standards.
2. Support of the University's ICT Infrastructure. This covers the management and day-to-day operation of the:
    a. Network Operating Centre.
    b. University's backbone network that interconnects the Local Area Networks (LANs) and Wide Area Networks (WANs).
    c. Computer laboratories (labs).
    d. IP Telephone system.

3. The setup, administration, troubleshooting and problem resolution of personal computers, printers, servers, networks and communications systems. The ICTD is responsible for:
    a. The University Email system.
    b. Internet access.
    c. Technical support of the University website.
    d. Promoting the use of e-learning tools.
    e. Basic ICT training for staff and students.
    f. ICT advisory services.
    g. Developing and generating reports.
    h. Technical support.

5.2 The Head of the ICTD (The ICT Director)

The ICT Director shall be responsible for the day-to-day management of the ICT.

5.3 The Planning and Quality Assurance Unit of the University

The Planning and Quality Assurance Unit of the University shall be responsible for:

1. The strategic planning, management of quality assurance as well as management of information systems of the University in consultation with the ICT Director.
2. Co-ordinating activities with the ICTD to ensure that the ICT facilities and services are managed and delivered at the highest level of quality.
3. Liaising with the ICTD to prepare and maintain an up to date database on staff and students as well as basic statistics in the University

5.4 The ICT Management Committee

The functions of the ICT Management Committee shall be to:

1. Formulate policies and guidelines for the running of the ICTD.
2. To provide oversight of the administration of the ICTD.
3. Make recommendations to the Senate on the use of ICT facilities in the University.
4. Offer advice on the development of ICT infrastructure and acquisition of computers and ICT equipment.

5.5 The ICT Help Desk

The ICT Help Desk shall be created by the ICTD and shall be the basis for managing problems and changes. Help Desk procedures shall be established for receiving user problems and requests, trouble ticketing and tracking, as well as problem resolution and escalation.

5.5.1 Objective

The objective of the ICT Help Desk is to provide customer-oriented ICT services to the NU user community by receiving problem calls, requests and enquiries, and arranging to have them resolved or addressed by the appropriate ICT personnel.

5.5.2 Service Availability

The Help Desk service shall be available during working hours. The Help Desk can be reached either through the phone number +23279453322 or Email: ict@njala.edu.sl

6 Service and Support

6.1 Structure

At the heart of the University's ICT structure is the ICT Directorate. The ICT Director is responsible for the day-to-day running of ICT services and for ensuring the priorities of work follow the agreed service level description.

The ICT Director is responsible to the Governing Body for all aspects of the University's ICT service, support and development. In addition, there is a Web Master who is responsible for the development of the University's websites and for web contents development and communications.

6.2 Support Priorities.

The Service Level Description (SLD) gives a detailed description of the service and support priorities currently employed by the ICT Directorate. A summary of the priorities which are ranked A to G:

A. The 1st priority is to ensure the IT infrastructure remains in operation; this includes both the network and servers. From time to time upgrades and developments to the network and servers will be necessary and will take high priority in order to minimise overall disruption and to accommodate on-site contractors.
B. The University Administration infrastructure is next; this includes supported departmental systems such as databases and related systems, also shared printers. [Priority for any one department will depend on time of year, so, for example, the Academic Affairs is given priority during the admissions and examination cycle; the Guest House and Domestic Bursary during the conference season and the Finance Department at the time of the Finance Director's report.]. Finally, within this category is equipment to be used for an imminent presentation within University.
C. Academic priorities: this includes support for Professors/Fellows and University Lecturers to ensure there is no serious interruption in the operation of their IT equipment
D. The University computer rooms: to ensure these remain fully operational with an ordering of: (a) the network integrity for an entire room, (b) breakdown of a printer or other peripheral device, where no alternative is available locally.
E. For the single-user: breakdown of an individual computer or other university-owned peripheral devices; software problems, major hardware problems affecting non-university owned equipment but being used for academic or university-related work.
F. Current students with critical problems involving their own personal PCs; single-user network or software problems.
G. Help and advice on equipment, software upgrades and general IT requests from Administrators and Lecturers.

Notwithstanding the above ordering it will be open to either the ICT Director or the ICT Staff Members to escalate a support request if it has consequences for the operation of an immediate University activity.

7 Security

7.1 Network and Computers

Security of our network and of the computers used for the administration of University business is a crucial aspect of our ICT-policy. For this reason, all computers attached to the network must have anti-virus software installed and in general should be checked before any connection is made to the network by the ICT department. Owners of personal computers are responsible for ensuring that their software is up-to-date in terms of security patches and anti-virus updates. In general, this will be configured automatically but owners must ultimately take responsibility for their own equipment. This includes care in the choice of passwords and in the use of email accounts. Breaches in security where this is due to inappropriate computer use will be viewed seriously by the University and could result in temporary exclusion from the network. In addition, the University shall develop its information security policy and, in particular, recognises that:
The University is committed to protecting the security of its information and information systems in order to ensure that:

1. the integrity of information is maintained, so that it is accurate, up to date and fit for purpose;
2. Information is always available to those who need it and there is no disruption to the business of the University;
3. Confidentiality is not breached, so that information is accessed only by those authorised to do so;
4. the University meets its legal requirements, including those applicable to personal data under the Access to information ACT or the Data Protection Act; and
5. the reputation of the University is safeguarded."

7.2 Firewall

The University network incorporates a firewall to control data traffic into and out of our local network; this increases the security of our network and helps to keep the threat of malicious attacks to a minimum and to keep confidential information secure.

7.3 Retention of Data

Anti-terrorism, crime and security law have implications for the data we retain with regard to digital communications. In brief, the Data Retention (EC Directive) regulations of 2009 require Internet Service Providers (ISPs) to retain data necessary to:

i. trace and identify the source of communication;
ii. identify the destination of a communication;
iii. identify the date, time and duration of a communication; and
iv. identify the type of communication.

In the words of the 2009 Regulations, this includes data generated or processed by means of `mobile telephony', `internet access', `internet email' and `internet telephony.' It is also necessary to identify the users' communication equipment.

8 Software

The University takes seriously breaches of software licence agreements and piracy with respect to software packages. For the purposes of the University's administration, computer software will be installed by the University's ICT Directorate; for students' personal computers software will be assumed to be bona_de and kept up-to- date with the latest security patches where appropriate (e.g. for Adobe Reader, Microsoft Office).

9 Procurement of IT Equipment

In general computers and other equipment used by the various University Offices are procured by the ICT Directorate. Computers used for administrative purposes have in general a common program suite to cover daily tasks as well as specific departmental software. Other additional software can be arranged through the ICT Directorate as necessary subject to the user's need in relation to their University duties. All new University computers will have appropriate anti-virus, anti-spyware and malware software installed, and generally software updates will either be automatic or organised through the ICT Directorate on a routine basis. Procurement of mobile devices (section 10) should be authorised by line managers giving business cases for each device requested; these should be set up and registered by the ICT Directorate. In ordering equipment for the University, the ICT Director will ensure that full use is made of educational and other discounts and will ensure that an up-to-date database (inventory) exists for all such equipment, including mobile devices; this is to ensure timely upgrades of equipment under the renewal policy and to assist in cases of theft leading to insurance claims.

10 The University Network

The University network comprises optical, wired and wireless connections through-out the various University sites. Switch gear and wireless access points are the property of the University and are maintained by the University for its administrative and academic pursuits. Only contractors engaged by the ICT directorate and the members of the ICT directorate shall have direct access to any hardware component of the network, and interfering with any part of the wiring, optical fibres and hardware by any University member will be deemed to be a serious matter.

11 Njala University Email Accounts and the Internet

To obtain a University/University email account a user first requires a University Staff or Student ID or Card. Once this has been issued an email account is automatically created by ICT Support Services; this will be of the form: first letter of Initial.Last@njala.edu.sl .While it is open to the University to set up an office name to cover, for example, general enquiries, this needs to involve the ICT directorate.

Other email accounts, available through outside providers, e.g., gmail, Hotmail etc., can be set up by individuals but accounts incorporating the University's name should only be used by agreement with the relevant line manager and ICT Staff; the ICT Directorate should hold all relevant details of the account including passwords which should be sufficiently strong to ensure necessary security. Such accounts should not be used in any way that attracts unauthorised cost or defamation to the University or University. Inappropriate use of email accounts or the internet may lead to sanctions and to suspension from the network.

As regards use of the internet, all students and visitors should read and sign the University's acceptable use policy.

Users are not permitted to use University IT or network facilities for any of the following:

1) any unlawful activity;
2) the creation, transmission, storage, downloading, or display of any offence, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the head of his or her department or the chairman of his or her faculty board (or, if the user is the head of a department or the chairman of a faculty board, from the head of his or her division);
3) the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Code of Practice on Harassment;
4) the creation or transmission of defamatory material about any individual or organisation;
5) the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;
6) the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;
7) the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;
8) the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;
9) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University; or commercial purposes (including advertising commercial services) without specific authorisation;
10) gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;
11) the deliberate or reckless undertaking of activities such as may result in any of the following:
    a) the waste of staff effort or network resources, including time on any system accessible via the university network;

b) the corruption or disruption of other users' data;

c) the unauthorised access, transmission or negligent loss of data;

d) the violation of the privacy of other users;

e) the disruption of the work of other users;

f) the introduction or transmission of a virus or other malicious software into the network;

12) activities not directly connected with employment, study, or research in the University (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation."

Please be aware that computers on a high bandwidth network such as ours are a prime target and new vulnerabilities are discovered every day. You are encouraged to keep your machine's protection software updated and to take great care when opening email attachments. The ICT team will advise you on sensible precautions as necessary.

12 Guidance on the Use of Emails

Use of electronic mail is both widespread and common throughout the University. While use email communication is of tremendous value there are, nevertheless, a number of potential pitfalls and all users should be aware of these when transmitting, receiving and storing such messages. Below some guidance is provided which both represents good practice and identifies some of the major risks.

12.1 Risks associated with Email Correspondence.

1. Emails carry the same weight of evidence as other types of written communication. Do not type anything which you would not be comfortable printing with a University letterhead since in the eyes of the law there is no difference.
2. Emails sent using University systems belong to the University and not to you as an individual.
3. Emails are legally enforceable. If you 'informally' agree to do something by email or use email to request goods or services, the email constitutes a contract.
4. Because email has the same legal status as a signed document on University letterhead, email exchanges for contractual discussions must be managed carefully, to ensure that there is a clear distinction between negotiating the terms and conditions of a contract, and agreeing them (and thereby entering into a contract).
5. Emails are legally disclosable. In response to requests under the Freedom of Information and Data Protection Acts, and following court orders, most information contained in an email is disclosable.
6. Email is not secure and is easily intercepted.

12.2 Inappropriate Use of Email

1. When transferring documents, particularly where you wish to make documents available to multiple recipients, email is not the most suitable means of distribution. For each person to whom the email is being distributed, a copy is stored in each of their email accounts, as well as in your own sent items folder. This is inefficient use of mail store quite apart from any security issues.
2. In situations where you need to transfer documents to others: the best practice is to place the documents in a location accessible to all of your recipients, whether this is an intranet, SharePoint or internet site, or your departmental networked file store. You can then email your recipients with details of the location.
3. When communicating about other members of staff (or students) you need to be mindful that under the Access to Information and Data Protection Acts, staff and students have a number of rights. This includes the right to access almost any information held about them by the University, including emails in which they are identified. This is a right which is increasingly being used in grievance/complaints situations. If you need to communicate potentially sensitive information (including communicating with HR), it is more appropriate to carry this out in person and (if need be) commit a summary of meeting notes in your own, non-work related, private diary/notebook.

13 Social Media

Social media accounts set up in the name of the University, or attributable to the University, can provide a fast route for feedback, comments and ideas. As such this facility provides a valuable forum for discussion. Unfortunately, it is open to abuse and can in extreme cases lead to reputational damage to the Institution or individual defamation of character and subsequent legal action. With this in mind, all University related social media accounts (facebook, twitter etc) should have a key administrator who takes responsibility for the account and who is responsible for granting write (administrator) access to the account. The University ICT Director is to be the key administrator on all such University accounts and should hold account details and any necessary passwords. As a general rule there is a need to be careful over copyright, trademarks, data protection and the use of logos. Also, in the interests of security users should avoid revealing personal information where possible, avoid any dialogue with journalists and avoid unsubstantiated claims.

14 Management of the University Websites

The University's websites are overseen by the ICT Committee Group which meets regularly during the academic year. There are currently representatives from the Quality Assurance, the Academic and Administrative departments. The Group is chaired by the ICT Director acting as secretary for the group. To ensure coherence across the site a protocol has been established which is given in Appendix H; the University ICT Director is responsible for ensuring compliance with relevant legislation and with the University's policies and standards regarding quality and presentation. This includes the accuracy of the content and ensuring that the site is kept up to date.

15 WiFi and VoIP

The University is aware of the growing use of mobile equipment and is expanding its WiFi provision accordingly for all members of University. Around the main campuses there are WiFi access points for connection to the University network. The University has set as a high priority complete coverage of the main site in the near future. In the immediate future, provision shall be made for voice over internet telephones (VoIP).

16 Mobile Devices

Mobile devices are becoming increasingly common and sophisticated. These range from tablet computers and iPads to smartphones. In what follows devices which use SIM cards of any description are included. The University only supports the acquisition and maintenance of mobile phones (including smartphones) and other mobile devices where a person's work requires the use of such devices. In these cases the choice of network (carrier) will be at the University's discretion using a corporate account. Use of such University-owned devices should be related only to calls and emails made in the context of University activities.

17 Transgressions / Penalties for Unacceptable Use

Where there is evidence of unacceptable use, the University may restrict or prohibit the use of its ICT resources. Violations of this policy shall be treated in accordance with applicable University Statutes, Ordinance, Rules and Regulations

In other cases involving a breach of security, or a charge of computer hacking, damage or improper use of equipment, or use of equipment that affects the entire University network, then the following sequence of events would be triggered.

1. The student would get an email from the ICT directorate.
2. The ICT Directorate would also be informed.
3. There will be an interview with the student either conducted by the ICT Director, the IT Director, or both depending on the nature of the breach. The student's account would be temporarily suspended, while the breach is investigated, usually for a period of 1-2 days.
4. If the breach is significant and further measures are necessary then the University Administration and Proctors are likely to become involved.
5. It will be up to the University Administration to impose a fine or a period offline or both quite apart from any University sanctions imposed by the Proctors.

18 Revisions to this Policy

It is anticipated, with the speed of development in IT equipment and infrastructure, that revisions may from time to time be necessary to this policy document. In the first instance it will be for the IT Director to bring forward such changes which will then go to ICT Committee for approval. In any case, the policy document will be reviewed annually and updated as necessary in the light of developments in the University.