KNUST POLICY 00--

Kwame Nkrumah University of Science and Technology, Kumasi

Information and Communications Technology POLICY

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

KWAME NKRUMAH UNIVERSITY OF SCIENCE
AND TECHNOLOGY, KUMASI-GHANA

**QUALITY ASSURANCE AND
PLANNING OFFICE (QAPO)**

ISBN: 978-9988-2-8487-9

Quality Assurance and Planning Office
Vice-Chancellor's Office
Kwame Nkrumah University of Science and Technology
KNUST, Kumasi
PMB UPO, Kumasi-Ghana

Tel: +233 322060319
Email: info.qapo@knust.edu.gh

Layout Design by
Frank Boadu, University Press, KNUST

Cover Design
Francis K. N. Nunoo, Department of Publishing Studies, KNUST

Foreword

The Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, is dedicated to using Information and Communications Technology (ICT) as a key tool to fulfill its primary mission and to recruit top talent staff, students, partners, and business.

ICT is currently a major factor in KNUST's primary operations, which include teaching, knowledge promotion, and service. Its function as the corporate foundation for effectively managing all university operations is well understood.

The KNUST ICT Policy was released on schedule. ICT Governance, Information Security Principles, IT Business Continuity and Disaster Recovery, Software Development, IT Support Services, Data Communication Network frameworks, and many other important IT areas that influence business operations in the environment will all be governed by the policy.

Benefits of using IT services properly in higher education include raising the standard of teaching and learning, expanding opportunities for graduate employment, improving international cooperation, student and staff capacity building, and raising the institution's profile.

The strategy and initiatives of Kwame Nkrumah University of Science and Technology to enhance its reputation, visibility, and appeal to its stakeholders both domestically and globally are reflected in this policy document, along with the steps that must be taken to stay relevant in the higher education sector.

PROFESSOR (Mrs.) Rita Akosua Dickson
VICE-CHANCELLOR KNUST

Acknowledgement

As part of the strategic planning mandate of the Quality Assurance and Planning Office (QAPO), University policies are initiated and proposed for approval by the Academic Board.

The Quality Assurance and Planning Office is grateful to the Committee consisting of Mr. Courage Julius Logah (Chairman), Mr. Abraham Brew-Sam, Mr. Kwabena Nyanteng, Mr. Kojo Ankar-Brewoo, Mr. Joachim Akute Azu, Mr. Phanuel Seli Asense, Mr. Stephen Kwadwo Osei, Mr. Richard Ansah, Mr. Abeaku Badu Arthur, Mr. Emmanuel Mfum-Mensah and Mr. Foster Sedem Kwame Dedume all of the University Information Technology Services (UITS) who provided inputs for this Policy. They are deeply appreciated for their enormous contributions.

We are equally indebted to the staff of QAPO and the Publication and Documentations Unit of the University Relations Office (URO) who facilitated the technical review and publication of this Policy.

Lastly, we wish to appreciate the contributions of all staff of the University who contributed in diverse ways to the development and approval of this Policy.

PROFESSOR Jerry John Kponyo
DEAN QUALITY ASSURANCE AND PLANNING OFFICE
March, 2025

OFFICIAL COPY CAN BE OBTAINED FROM:
Telephone Number: 0322060319
E-mail: info.qapo@knust.edu.gh

Preface

Information and Communications Technology (ICT) has become a key driver for the core business of KNUST – Teaching, Promotion of Knowledge, and Service. Its role is recognized by the University Strategic Plan (PLAN2K16-25). ICT will be used as the corporate backbone to efficiently run all processes of the University and will be intrinsically involved in shaping and developing institutional strategy to enhance the competitive advantage, effective administration, academic excellence, and visibility of the University.

ICT will be used as a tool to effectively realize the Vision, Mission, and Strategic Priorities of the University.

Contents

GENERAL INFORMATION

Overview of the University

The Kwame Nkrumah University of Science and Technology (KNUST) was founded to provide higher education with special reference to science and technology and to act as a catalyst for the technological development of the country.

The University has its main campus at Kumasi and several satellite campuses all over Ghana. The academic activities of KNUST are performed by six colleges and the Institute of Distance Learning. The six colleges are: College of Agriculture and Natural Resources, College of Architecture and Built Environment, College of Humanities and Social Sciences, College of Engineering, College of Health Sciences, and College of Science.

The Principal Officers of the University are the Chancellor, the Chairman of the University Council and the Vice-Chancellor. The Vice-Chancellor is the academic and administrative head of the University and the chief disciplinary officer.

The University has, within the period of its existence, become an important center for the training of scientists and technologists not only for Ghana but also for African countries and other countries, especially of the European Union and North America.

Vision and Mission of the University

Vision

To build on KNUST's leadership as the premier science and technology university in Ghana and to be among the top ten Universities in Africa.

Mission

KNUST exists to advance knowledge in science and technology through creating an environment for undertaking relevant research, quality teaching, entrepreneurship training and community engagement to improve the quality of life.

ICT Objectives of the University

The increasing role of Information and Communications Technology (ICT) as a vehicle for teaching, learning and research, and as an important key skill for everyday life, has led to ICT moving towards the core of the University's work as well as responding to the Vision, Mission, and strategic objectives of the University. The University's ICT policy and the development plan is meant to contribute to the realisation of the national ICT aspirations for education and national development. To this end, the University's ICT Policy seeks to achieve the following objectives:

- To extend ICT services to all Units of the University
- To ensure the availability of User-level Communication Services.
- To develop schemes for the growth and financial sustainability of ICT resources through appropriate funding and operational mechanism.
- To ensure sustainable management of the university's ICT resources through the creation of appropriate institutional framework.
- To develop content management and information systems for the University.
- To regularly train all students and members of staff to equip them with the requisite skills to fully exploit the ICT environment in their different functions.

ICT GOVERNANCE

ICT Governance deals with the processes that are employed to ensure the effective and efficient use of ICT to achieve corporate goals as well as to monitor and control key information technology capability decisions to ensure the uninterrupted delivery of value to key stakeholders in an organization. Technology has become paramount in our transformation agenda, but its use comes along with significant risks.

Due to its increase in prominence and associated risks, ICT governance is recognized as the ultimate responsibility of the KNUST Council and Management.

University Information Technology Services (UITS)

- UITS will be recognized as the main provider of central ICT services across KNUST and plays a leading role in the development of ICT in teaching and research.
- UITS must continue to offer high-quality services that meet the requirements of users in the most cost-effective way and must identify new services while maintaining existing ones.
- UITS must have appropriate funding to offer and develop the existing range of services, but also to be flexible enough to bring in new services as required. In this regard, a special UITS development fund should be set up to fund activities of the unit. Special levies should be deducted from research projects which make use of ICT services into the fund. The objective of this fund is to support continuous research into ICT and its development and the development of UITS staff.

- UITS must also be able to offer a core set of reliable services and, where desirable, enhanced services which are charged on a cost-recovery basis.
- It is a policy of the university to make UITS a self-accounting unit with a permanent building and other ancillary facilities for the unit.
- UITS shall be responsible for the acquisition, development, deployment, utilisation and disposal of all ICT services and equipment in the university in a way that is environmentally sustainable.

Core ICT Management

University Information and Communications Technology Management Committee

Composition

1. Pro Vice-Chancellor
2. Registrar/Representative
3. University Librarian
4. Finance Officer/Representative
5. Director of University Information Technology Services
6. SRC President / Representative
7. Deputy Directors of UITS
8. Head, Department of Computer Science
9. Head, Department of Computer Engineering
10. Snr. Assistant Registrar, UITS (Member/Secretary)

Functions

- To advise the University on the present and future development of information and communications technology.

- To formulate and regulate ICT policies and strategies in line with the university's core business.
- To Monitor and control the progress of all activities arising from the implementation of the University's ICT Policy.
- To make, amend, and publish regulations, subject to approval by academic board, for the control, management, and security of the use of the University's ICT facilities.

Meetings and Quorum

The Committee shall meet at least once a year, and the quorum shall not be less than one-half (1/2) of its total membership.

University Information Technology Services (UITS) Management Board

Composition

1. Chairman, a senior member, appointed by the Vice-Chancellor.
2. Director of UITS
3. Deputy Directors of UITS
4. Snr. Assistant Registrar (Administrative Manager)
5. Snr. Accountant (Finance Manager)
6. One representative from each College
7. Representative of University Librarian
8. Representative of the Institute of Distance Learning
9. President or his representative (Student Representative Council)
10. President or his representative (Graduate Student Association)

Functions

The Board shall be responsible for the strategic oversight of the operations and budget of the UITS, which shall include:

- To advise and instruct the Director of the University Information Technology and Services (UITS) as required for the Director to fulfill the duties of his or her office; and
- The Board shall report at least once every year to the ICT Committee and bring to the committee's attention new policy issues relating to its remit.

INFORMATION SECURITY POLICY

It is KNUST's responsibility to ensure the Confidentiality, Integrity and Availability of information and information systems always. To this end, measures will be put in place to prevent unauthorized disclosure of information, alteration of data and denial of access to systems and data. Information assets in all forms and throughout their life cycle will be protected through information management policies and actions that meet applicable regulations, laws, and contractual requirements to support the University's mission, vision, core values and philosophy. KNUST will develop, deploy, and maintain countermeasures that physically protect people, equipment, data, and the facilities that house these.

KNUST will as much as possible follow the Centre for Internet Security (CIS) Controls which are top priority controls that provide a defense in depth strategy implementation and counteract the most common attacks on information security.

The purpose of the Information Security Policy is to ensure the protection of all information and information assets of the university from unauthorized disclosure of information, alteration of data and denial of access to systems and data.

All staff who develop and maintain information systems and assets and all third parties who provide information systems or connect to university information systems must ensure compliance to the principles of the Information Security Policy.

Policy Principles

1. Inventory and Control of Hardware Assets. Maintenance of an asset list of authorized hardware; the authorization of all hardware that connects to the university network; making use

of tools such as IP address management tools, DHCP logging, discovery tools or such other tools to identify all hardware assets and to update the hardware asset inventory.

2. Inventory and Control of Software Assets. Maintenance of an asset list of authorized software and the authorization of all software, software libraries and scripts that execute on university systems making use of whitelisting technology.
3. Continuous Vulnerability Management. Making use of vulnerability scanning tools that are Security Content Automation Protocol (SCAP) compliant to automatically scan the university network on a regular and frequent schedule and the provision of automated software update tools for all operating systems and all third-party software.
4. Controlled Use of Administrative Privileges. Control of administrative privileges to ensure that only authorized individuals have elevated privileges; giving users with elevated privileges their own personal accounts, which are different from administrative accounts, making use of encryption and multifactor authentication for administrative access, segmentation and dedication of machines used for administrative access and restriction of access to scripting tools; enhancement of the security of passwords by adhering to the rules for strong password protection such as minimum password length and complexity and ensuring that no new hardware or software assets are deployed with default passwords.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. Maintenance of standard security configurations, management tools for all approved software, operating systems, maintenance, storage of secure images and templates for all systems based on approved configuration standards.
6. Maintenance, Monitoring and Analysis of Audit Logs. Management of logging by ensuring the enabling of local logging on all systems and network devices, the aggregation

of all logs to central log management systems and the review and analysis of logs on a regular basis and the use of a Security Information and Event Management (SIEM) system or log analytic tools for log analysis.

7. Email and Web Browser Protections. Management of web and email security by ensuring that only fully supported web browsers, email clients along with their corresponding authorized plugins, add-ons and scripting languages are allowed to execute in the university and making use of sandboxing to block malicious email attachments; and restricting access to unapproved websites by making use of network-based URL filters and employing the use of DNS filtering to block access to known malicious domains.

8. Malware Defenses in this document refers to making use of centrally managed corporate antimalware software that continuously monitors and scans all systems installed as well as removable media when connected. It is configured to block auto-run of removable media content and enables operating system anti-exploitation features as a way of protecting systems and user data.

9. Limitation and Control of Network Ports, Protocols, and Services. Dropping all traffic except those that are explicitly allowed to all ports, protocols, and services by making use of host-based firewalls or port filtering tools with default deny rules.

10. Data Recovery Capabilities. Automatic backup of complete system data through processes such as imaging and the testing of data integrity of backups on a frequent schedule.

11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches. Installation of the latest stable versions of security updates on network devices and standard security configurations of these devices.

12. Boundary Defense. Ensuring boundary defenses by maintaining an inventory of university network boundaries, allowing only specific necessary or trusted IP ranges through these

boundaries, and regularly scanning from outside these trusted zones to detect any unauthorized access across these boundaries; use of intrusion detection and intrusion prevention systems to monitor and detect unusual behaviour or attack mechanisms and to block and alert of these at each university boundary.

13. Data Protection. Maintenance of an inventory of sensitive information and segregation or isolation of critical systems from the regular network and the use of encryption of whole disks for university mobile devices such as laptops, encryption of USB storage devices while at rest and encryption of sensitive data in motion.

14. Controlled Access Based on the Need to Know. Controlled access to information such that only individuals with a need to access specific information are granted access to them by making use of techniques such as claims and access control lists.

15. Wireless Access Control. Controlling wireless access by maintaining an inventory of all authorized wireless access points and detecting and alerting of any unauthorized wireless access points connected to the university network by making use of wireless intrusion detection systems or appropriate network vulnerability scanning tools and ensuring that wireless networks make use of appropriate authentication protocols.

16. Account Monitoring and Control. Controlling and monitoring accounts by maintaining an inventory of all accounts, setting up and maintaining a system for the effective grant or revocation of system access when required, and alerting when attempts are made to enable previously disabled accounts, proper storage, transmission, management, protection of authentication credentials, logon sessions and behaviour.

17. Implement a Security Awareness and Training Program. Creation of an awareness program of information security for all employees to complete on a regular basis to ensure understanding and competency in set minimum levels of information security. Training of staff on information security

to enable identification of threats, attacks, and appropriate dealings with sensitive information.

18. Application Software Security. Establishment of secure coding practices for software development, ensuring training in secure coding for software development staff, maintaining separate production, non-production environments for systems, security of applications and databases using application specific firewalls, web application filters and hardening configuration templates for databases. Incident Response and Management. Incident response planning, management, and testing.
19. Penetration Tests and Red Team Exercises. Establishment of programs for and conducting regular and comprehensive internal and external penetration testing.

Computer Emergency Response Team

A Computer Emergency Response Team is set up by this policy and they shall be responsible for all Cyber Security Emergencies. The composition of the team is as follows:

1. Director, UITS
2. All Deputy Directors
3. All Senior Members, Information Security & Technology Assurance Division

PASSWORD POLICY

A crucial aspect of ICT Security, Data Governance and Business Continuity is establishing and enforcing a strong password policy. A password-protected system is only as secure as the weakest password that has access to it. In view of this, passwords and their management are crucial to ICT security. A poor password may lead to the compromise of all Kwame Nkrumah University of Science and Technology (KNUST) electronic systems and data. It is therefore imperative that all KNUST employees and users with access to KNUST systems adhere to the guidelines in this policy document to select and secure their user passwords.

The purpose of the Password Policy is to establish a standard for the creation of strong passwords and their protection.

The Password Policy is applicable to all staff of KNUST who are responsible for one or more accounts or any user with access to any KNUST resource that requires a password. Failure by staff and users to comply with the terms of this policy may lead to KNUST taking disciplinary action against such staff and users.

Policy Principles

i. All systems-level passwords must be changed at least every 90 days.

ii. All user-level passwords must be changed at least every 180 days and avoidance of same password reuse.

iii. The default administrator user account should be disabled, and a new local administrator account created. Users should be logging in with their own accounts.

iv. Never use one account for multiple users.

v. Temporary credentials sent to users must, as much as possible, expire after 24 hours.

vi. User accounts access should be revoked/disabled immediately a staff or user ceases to work for KNUST.

vii. User accounts to specific systems should be disabled immediately a staff or user no longer requires the access.

viii. Default passwords shall be changed immediately on all equipment and systems.

ix. All devices capable of being password protected should be password protected. E.g., manageable switches, routers, servers, desktop computers, laptops, smart devices, and wireless access points.

x. Use multi-factor authentication (MFA) whenever the systems in use allow it. This may involve a two-step verification process which requires the user to use an additional factor—be it a fingerprint, physical security key, or one-time password—before they can access an account.

xi. Any device that accesses the internet is at risk of e-Crime. Ensure that all such devices including smartphones and tablets have antiviruses installed that update regularly. Always use the official app store when downloading apps onto your smartphone or tablet.

Guidelines

Password construction requirements:

i. Passwords should be a minimum length of eight (8) characters and contain at least one upper case letter one lower case letter, one number and one special character on all systems.

ii. Passwords should not contain a dictionary word or proper name especially your name, your company name, your mother's maiden name, your children's names, or the name of your favourite sports team.

iii. Non-English words are harder to guess so use them particularly local dialect words such as Akan, Ga and Ewe words.

iv. Passwords should not contain easily acquired personal information such as your year of birth.

v. You should create unique passwords for each account. Failure to do this would give a hacker who gets one password access to all your accounts.

vi. Do not write down your password. To remember passwords, create passwords by picking a phrase, taking its initials, replacing some of those letters with numbers, other characters and mixing up the capitalization. E.g., "I love KNUST for its excellent service" becomes iLk4le$!

vii. Passwords should not be the same as the User ID.

viii. Passwords should expire within a maximum of 90 calendar days.

ix. Passwords should not be identical to the previous passwords used on an account.

x. Passwords should not be transmitted in the clear or plaintext.

xi. Passwords should not be displayed when entered.

xii. Ensure passwords are only reset for authorized users.

xiii. Every computer on the network, including home computers that are used to access the network remotely, must have enterprise-level security programs installed and updated.

User Account Deactivation

When an access level is no longer needed, the following procedures should be followed:

i. The user concerned should notify his or her immediate supervisor.

ii. The supervisor should notify UITS by email. Supervisors should do this even for situations where the user concerned does not inform them, but they become aware that the user's access level is no longer needed.

iii. UITS will then disable the user's account.

Password Protection Standards

All passwords are to be treated as sensitive and confidential KNUST information.

The following general guidelines apply:

Do nots

i. Do not use your User ID as your password.

ii. Do not use passwords like "password," "passwordl" and "Pa$$word".

iii. Do not share KNUST passwords with anyone, including administrative assistants or secretaries, Teaching Assistants, etc.

iv. Do not reveal a password over the phone to anyone.

v. Do not reveal a password to your boss.

vi. Do not ask your subordinate for his/her password.

vii. Do not talk about your password in front of others.

viii. Do not hint at the format of a password (e.g., "my family name")

ix. Do not reveal a password on questionnaires or security forms.

x. Do not share a password with family members.

xi. Do not reveal a password to a co-worker while on vacation.

xii. Do not use the "Remember Password" feature of applications.

xiii. Do not write passwords down and store them anywhere in your office.

xiv. Do not store passwords in a file on any computer system unencrypted.

xv. Do not use a password for a KNUST account that you already use for a personal account.

xvi. Do not use a password manager or other tools to help store and remember passwords without the permission of UITS.

Dos

i. Report to the UITS if someone requests for your password.

ii. Report to the UITS if an account or password is suspected to have been compromised and change passwords to such accounts immediately.

Password Theft

Employees should take steps to avoid phishing scams, trojan attacks, and other attempts by hackers to steal passwords and other sensitive information. All employees should receive training on how to recognize these attacks and must ensure they use anti-virus software, which is constantly updated.

Penetration Testing

A security auditor will periodically test systems for vulnerabilities. If your password is guessed or cracked during one of these tests, you will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Applications should, as much as possible, support authentication of individual users and not groups.
- Applications should not store passwords in clear text or in any easily reversible form.
- Applications should provide role management for assigning users to security levels.

Remote Access Users

Access to KNUST's networks via remote access is to be controlled by using either a Virtual Private Network (VPN) or a form of advanced authentication.

BUSINESS CONTINUITY AND DISASTER RECOVERY

In the event of a disaster, there is the need to ensure continuation of the business of KNUST and the quick and efficient recovery from the disaster. This is the purpose of the business continuity and disaster recovery plans.

The purpose of the Business Continuity Plan is to ensure continuation of the business of UITS and KNUST in the event of a disaster while the purpose of the Disaster Recovery Plan is to ensure speedy restoration of the services of the UITS and KNUST in the event of a disaster.

Business Continuity Team

An ICT Business Continuity Team is set up by this policy and they shall be responsible for planning to ensure continued provision of ICT services to KNUST after a disaster, possibly by operating from a different location or making use of alternate tools and processes. The composition of the team is as follows:

1. Director, UITS
2. All Deputy Directors
3. Representatives from the various Divisions

Disaster Recovery Team

An ICT Disaster Recovery Team is set up by this policy and they shall be responsible for restoration of normal provision of ICT services to KNUST after a disaster. The composition of the team is as follows:

1. Director, UITS

2. All Deputy Directors
3. Representatives from the various Divisions

Functions

The ICT Business Continuity and ICT Disaster Recovery Teams are to ensure the following:

1. Specification of emergency response procedures such as assessment of disaster and procedures for ensuring the notification and safety of personnel.
2. Specifying procedures for backup and offsite storage of data.
3. Data processing continuity planning involving continuing ICT data processing functions in the event of a disaster by making use of secondary processing sites.
4. Maintenance of requisite documentation for every critical business process or machinery.
5. Software escrow agreements for vendors to ensure safety and availability of software code should the vendor's business collapse.
6. Procedures to ensure accurate communication of facts on a disaster to the press, customers, and the public.
7. Procedures to ensure availability of backup utilities such as backup power.
8. Availability of important supplies and logistics.
9. Procedures for alternate means of firefighting should water supply be cut off such as making use of inert gases.
10. Plans for salvage and restoration of facilities and equipment.
11. Ensuring financial readiness by making use of such tools as insurance, standby assets, pre-purchased assets, cash reserves, establishment of lines of credit and establishing legal agreements say for the use of nearby facilities in the event of a disaster.

To this end, the ICT Business Continuity and ICT Disaster Recovery Teams are to ensure the following activities are carried out at a predetermined and regular interval:

1. Creation and update of Checklist of activities to carry out in the event of a disaster.
2. Structured walkthrough of the plan elements.
3. Simulation of disaster, which does not involve an actual recovery.
4. Running a parallel recovery test, which involves performance of an actual recovery using parallel systems.
5. Interruption or cutover recovery test, which shuts down or disconnects the production systems and performs a failover or switchover to the recovery systems (Chaos Engineering).

SOCIAL MEDIA POLICY

The University recognises that the effective use of social media can bring significant and measurable benefits to the University which include:

i. Enhancing the University's visibility, brand, and culture

ii. Improving the national and international reach of the University

iii. Improving stakeholder engagement and interaction

iv. Attracting high quality staff and students.

v. Ensuring cost-effective means of mass communication.

vi. Facilitating effective dissemination of research related information.

vii. Facilitating effective crisis communication.

viii. Showcasing the academic excellence of experts in various fields within the University

ix. Highlighting the achievements of the University and its alumni

Social media can be a risky space and comes with the risks inherent in managing a two-way communication tool that is dynamic and unlimited in scale. These include the risk of reputational damage, exposure of confidential and sensitive information, exposure of private information, use of abusive language, etc.

Policy Principles

Professional use of social media

KNUST employees using social media in a professional capacity, either through a Professional KNUST account or a Professional Personal

Account, should make sure that the communication adheres to the following 'Dos' and 'Do Nots':

Do Nots

i. Do not Link to content that could bring KNUST's name into disrepute. Always check that content that you share from other sources do not link to undesirable content.

ii. Do not Post a personal view using a Professional KNUST social media account. Always check to make sure which account you are signed into before posting.

iii. Do not Post comments that might be construed to be defamatory, discriminatory, offensive, harassing, hateful, racist, sexist, or obscene.

iv. Do not Publish confidential content.

v. Do not Breach data protections, privacy, copyright, or any relevant laws. It is better to link to third party content than to copy it to avoid copyright infringements.

vi. Do not Use inappropriate language and expressions.

vii. Do not Breach the terms of service of the social network in use.

viii. KNUST social media accounts should not be used for any private business or financial transactions including revenue from advertising, nor should any staff with administrative responsibilities realize any personal monetary profit from KNUST social media sites.

ix. KNUST social media accounts should refrain from posting content and liking or following users or pages that reflect personal interests.

Dos

i. Use professional, courteous, and respectful tone always

ii. Ensure permission to share all content and acknowledgement of authors of content.

iii. Check with the University Relations Office before publishing content that may generate controversy for KNUST.

iv. Think carefully before posting and responding to comments. When in doubt, get a second opinion.

v. Always proofread your comments before posting to ensure posts are free of spelling and grammatical errors. Ideally, a colleague should always review posts before being posted finally.

vi. Report any mistakes made while using social media to the University Relations Office.

vii. Make sure that passwords to KNUST social media accounts are adequately complex, protected and conform to the University's Password Policy.

viii. Ensure that devices that are used to post content on KNUST social media accounts, should not be left unattended. If any such device is lost, all logins to social media accounts contained on the device should be changed immediately and the incident reported to the Information Security Team and respective heads of college/department/unit.

ix. Should a KNUST social media account be hijacked, the University Information Technology Services should be brought in immediately to remedy the situation.

x. Check comments to your post and remove comments that violate this policy.

xi. Take steps to reduce barriers to access for individuals with disabilities.

xii. Ensure the accuracy of your content and that it is not misleading.

xiii. Official University style guidelines must be followed on all KNUST social media channels. These guidelines are outlined and detailed in the University Style Guide, which is maintained by the University Relations Office.

xiv. If you unintentionally post something online that is incorrect, correct it visibly and publicly as quickly as possible.

xv. Respond to enquiries as soon as possible.

xvi. Speak in first person plural.

xvii. As much as possible use the active rather than passive voice.

xviii. As much as possible use a semi casual tone, without using slangs or jargons.

xix. Check for new queries and respond a few times in a day. Replies need not be instant but should be made in a timely fashion.

xx. As much as possible responses should be short and link to the relevant information on appropriate KNUST website.

xxi. Avoid creating the impression that a user asked a foolish, irrelevant question or a question that the user could easily have found elsewhere. Direct the user to the appropriate University pages that provide answers.

Personal use of social media

Staff of KNUST who use personal social media accounts are to ensure that the communications adhere to the following 'Dos' and 'Do Nots':

Do Nots

i. Do not Link to content that could bring KNUST's name into disrepute.

ii. Always check that content that you share from other sources do not link to undesirable content.

iii. Do not Use university brand materials such as KNUST logos, trademarks, etc.

iv. Do not Post comments that might be construed to be defamatory, discriminatory, offensive, harassing, hateful, racist, sexist, or obscene.

v. Do not Publish confidential content of the University.

vi. Do not Use social media to air internal KNUST grievances.

vii. Do not Breach data protections, privacy, copyright, or any relevant laws. It is better to link to third party content than to copy it to avoid copyright infringements.

viii. Do not Use inappropriate language and expressions.

ix. Do not Breach the terms of service of the social network in use.

x. Do not Make comment that creates the impression that you are authorised to speak as a representative of KNUST or seeks to present your view as the official position of KNUST on a matter when you are not authorised to do so.

xi. Do not Impersonate another individual on social media.

Dos

i. Use a disclaimer when your profile or comments indicate that you are a staff of KNUST. Disclaimers can be put on your profile or placed after posts.

ii. Express opinions but do so in a balanced and measured manner

iii. Ensure you have permission to share all content and acknowledge authors of such content.

The University does, however, recognise Academic Freedom whereby staff shall have freedom within the law to question, test received wisdom, to put forward new ideas, controversial or unpopular opinions, without placing themselves in jeopardy of losing their jobs or privileges.

DATA COMMUNICATION NETWORK POLICY

The Data communication Network

The data communication network provides the essential links between users of information and sources of information. The University shall establish a University-wide data communication network consisting of the following building blocks:

- A data network backbone inter-linking all buildings for each University campus. The following functional requirements shall guide the technology option used:
  - Highest speeds, reliability, efficiency, ease of maintenance and sustainability.
  - Inter-campus connections between the different sites of the University.
  - Options for either owner or leased links shall be considered whenever a procurement choice is to be made.
- Individual Local Area Networks for all administrative and Academic buildings at each University campus. Every staff shall have provision for network access at a workspace and every student computing facility shall be linked to the backbone.
- Infrastructure for wireless access within students and staff residences on the various campuses.
- Infrastructure provisions for off-campus access for both students and staff.

It is the policy of the University to promote ubiquitous, equitable access to ICT resources for students and staff to the network through the establishment of network infrastructure in all work areas of students and staff.

The Data Centre (DC)

The Data Centre shall be the home for all back-end servers and related equipment that provide the hardware platform on which all the central network services shall be run. It shall also be the major switching point for the data communication network. The University will maintain its Data Centre(s), specially designed with cooling, uninterruptible power supply, backup-facilities, physical protection, and smart access control. To assure a quick turn-around time in case of disasters, a Disaster Recovery Centre (DRC) shall be established at a remote location.

It is the policy of the University that all services that are common/shared by the University community are centrally hosted in the DC.

User Computing Resources

These consist of computing devices and related accessories the University community uses to access the various network services and to facilitate work.

It is the policy of the University to provide adequate computing time for each student and staff through the provision of sufficient computing facilities and access times. Computing resources are categorized into two groups.

Staff computing resources.

Computing resources to enhance staff operations shall be provided in one of two ways. The University shall either provide a computer at each staff desk or a centralized pool of computer resources accessible to all staff members based on needs assessment. However, the following category of staff shall be provided with computers: Senior Members, ICT Staff.

Student computing resources

Setting up of central computing centres like computer labs in Units and computer kiosks shall be the focus for student access. The University shall also explore possibilities of loan schemes for student ownership of computers to ease the load on this pool of facilities.

For both categories of users, wireless network access shall be made available within various campus locations where users can comfortably access ICT services. Focus shall be in residential premises and public buildings like the library.

Smart Access Infrastructure

Within the context of this policy, the rationale for smart access systems is to increase security of access to university resources. The End-User Smart access systems will provide security and access to different service units of the University. The university shall promote the use of smart access to special ICT services.

It is the policy of the University to manage access control to high security locations on the various campuses through the implementation of a smart access system.

SOFTWARE DEVELOPMENT AND ACQUISITION POLICY

For each ICT service or application, the UITS will take the decision whether it should be developed 'in-house' or acquired from external sources based on the following key considerations. Key factors that favour the decision to develop software should include the following:

- A customised ICT application or service that is totally responsive to the institution's very specific needs.
- Increased ease in developing software due to the growth of Rapid Application Development tools and systems.
- Ease of adapting software to rapidly changing user needs without having to co-ordinate the requirements with vendors.
- Developing professional competence in software development.
- Having sufficient internal IT resources and skills to develop software in-house

Key factors that favour the decision to acquire software should include the following:

- Ability to gain access to specialised skills that cannot be retained or for which there is insufficient need to have continuously available.
- Building software is still extremely costly.
- Insufficient staff and skills to develop specific software in-house.
- Ability to make short-term commitment for ICT development support instead of having to make major investment in staff recruitment and professional training.

INFORMATION SYSTEMS POLICY

All information systems would be developed or acquired to provide efficient systems for the storage, retrieval, processing, and analysis of relevant data aimed at streamlining and enhancing business processes and to provide the needed information for management decision and action. As much as is practicable, all manual procedures of recording and processing data would be automated and managed with an appropriate information system.

Administrative Systems:

The University shall automate its core administrative functions by establishing three main integrated information systems targeted to address the Finance, Human Resource and Student Records Management functions. All other information systems would interact with these systems as required to provide an enterprise view of all KNUST information for management action.

Student Information System (SIS)

The University will ensure that student academic records are efficiently and effectively managed through the establishment of a Student Information System (SIS). The system shall provide for proper storage, retrieval, and manipulation of student personal, academic, admission and financial data. Processes should be put in place to ensure that students records are stored and accessed safely.

It is the policy of the University to ensure efficient and effective management of student academic affairs using an integrated Student Information System.

Financial Management Information System (FMIS)

The University will ensure the effective and efficient management of its financial data through a Financial Information System which will enable the collection, storage, and analyses of university financial data. The Information System will support and improve cash collection, debt management, project management, budgets preparation, ledger management, accounts payable and receivable including other accounting functions. This will enable the university to make good financial management decisions in budgeting and financial forecasts saving the university money.

It is the Policy of the University to ensure that financial management processes and reporting facilities at both central and faculty levels are streamlined using an integrated Financial Information System.

Human Resource Management Information System (HRMIS)

A Human Resource Management Information System will be implemented in the University to enable the effective and efficient management of the human resource functions through capturing of personnel information and manipulating it to handle the administrative needs of the Human Resource Management Division. This will assist the university to manage the recruitment, orientation, training, appraisal, and pension fund administration of employees effectively and efficiently through use of the data that is captured by the information system.

It is the Policy of the University to enhance and streamline the human resource management and administrative processes using a Human Resource Management Information System.

Other Information Systems

The following information systems are recognized as relevant information systems which interact with the three core Administrative Systems identified above.

1. Library Management Information System
2. Hospital Management Information System

Technology Choice

The right technology, platforms and tools should always be chosen for the development and management of information systems with an eye on security, efficiency and ease of use. The following platforms for applications are listed in order of preference:

1. Mobile apps
2. Web apps
3. Desktop apps

All technologies for development such as use of C#, Java, PHP, SQL etc. are acceptable for use once they satisfy the criteria of security and efficiency. Free and open-source software should always be considered and chosen where appropriate.

ICT SUPPORT SERVICES AND MANAGEMENT POLICY

The UITS shall provide support for all areas under the University network, computing devices, hardware, software, and implementation of ICT initiatives at all campuses and their related technical needs. The objective is to define and implement an effective ICT Service Management and Support approach that is aligned to the Vision of the University's Strategic Plan.

Policy Principles

Roles

a) The University shall define and implement an appropriate ICT Service Management process and procedure aligned to the goals and objectives of the University

b) The UITS shall define and implement a Business Model for the provision of ICT services to external clientele.

c) The UITS shall additionally setup/operate a business unit that shall generate resources to improve the welfare of its personnel.

ICT Services Support

The ICT Services Support will be defined as such operations carried out by authorized personnel to ensure efficiency, stability and continuity of any ICT service or equipment to ensure it meets its intended user requirements. In line with this, this policy will apply to all University owned ICT applications and devices.

Responsibilities of ICT Services Support personnel

The ICT Services Personnel (system administrators, ICT Lab attendants, ICT technicians, Web administrators) employed by the University within all Departments and Colleges shall functionally report to the Unit responsible for ICT, the UITS. Accordingly, the University shall provide the necessary work tools, safety gear and training for all ICT services support personnel. Accordingly, such personnel shall:

a) Ensure protection mechanisms exist against ICT devices tampering, alteration or theft.

b) Ensure ICT protection controls exist to safeguard security of systems and information.

c) Provide assistance and guidance towards compliance of ICT policies.

d) Provide technical support in line with approved ICT procedures for any system, service, device downtime or breach.

e) Ensure installation and configuration of all hardware and software is aligned to approved ICT standards.

f) Ensure safe custody and authorized usage of all University software licenses, copyright and usage keys.

END USER SKILL DEVELOPMENT POLICY

End users are the University employees and students who make use of the available ICT resources, and they generally fall into two categories: students and staff. End user skills must be developed so that all users are able to:

- Use ICT services and systems effectively and as independently as possible
- Contribute to the specification, design, and implementation of ICT applications.
- Be aware of the shared responsibilities for equipment, software, data and enforce an atmosphere of collective responsibility and system ownership.
- Manage and control complex project-oriented processes, like implementing University-wide infrastructure or information systems.
- Establish and sustain the effective use of available ICT resources for academic, administrative, or managerial tasks.

Basic ICT Skills

Students shall be made ICT literate during their time of study at KNUST. The Department of Computer Science shall develop a standard cross-cutting basic ICT skills course which should be adopted and administered by all University units. The Department of Computer Science shall be required to vet the lecturers who teach this course in each unit and it shall also carry out the monitoring and evaluation function.

It is the Policy of the University to ensure that all students take the introductory basic ICT skills course at the beginning of their training and are provided with progressive and continuous ICT training courses that are tailored to their specific academic programmes.

Staff shall be trained on a continuous basis to build their ICT expertise and experience. This will ensure that they are competent enough to use the University's ICT resources to enhance the University's core business (i.e., teaching, learning, research, and administration).

Academic Specific Skills

Although the Quality Assurance and Planning Office is mandated to oversee the development of academic programmes in the University, each academic and research unit shall be required to develop progressive and continuous ICT courses that are tailored to their specific academic disciplines. This will ensure that students apply ICT skills throughout their learning experience.

It is the Policy of the University to ensure that students are provided with progressive and continuous ICT training courses that are tailored to their specific academic programmes.

Administrative Skills

Staff should be able to understand and use the core University administrative applications such as the human resource management information system. The Human Resource Division shall develop and implement training strategies that help staff to make use of all the functions provided by the applications that are relevant to their work.

It is the Policy of the University to provide staff with training that equips them with the necessary skills to fully utilize the core administrative applications.

Library Services

The University Library makes use of ICT to provide access to a wide range of electronic information from both University and external sources. The end users shall have the information literacy skills to effectively use the electronic information which include electronic journals, databases, and other resources.

The University Library shall organize and conduct training that will:

- Create awareness about the wide range of available information resources
- Equip users with skills for determining their information needs
- Provide users with the ability to locate and retrieve relevant information
- Enable users to evaluate information and its sources
- Facilitate users' understanding of ethical and legal issues surrounding information use.

It is the Policy of the University to ensure that end users are provided with training that enables them to effectively utilise electronic information resources.

E-learning Skills

E-Learning describes learning done at a computer which is usually connected to a network, giving users the opportunity to learn almost anytime, anywhere. Development of e-learning skills assures appropriate and effective application of e-learning to teaching and improves student learning.

The E-learning Centre shall develop training packages for both staff and students and put in place evaluation and support mechanisms to ensure quality assurance of materials. This unit shall also set up an e-learning laboratory to develop local capacity in development and evaluation of appropriate training software.

Academic staff members shall continuously make use of e-learning to enhance the effectiveness of their teaching and provide students with an e-learning experience throughout their programmes of study. It is the policy of the University to ensure that students take introductory e-learning module(s) that is mandatory and continually use e-learning in their different programmes of study.

It is the policy of the University to provide staff with training so that they can adopt e-learning technologies and develop their e-learning skills.

ACCEPTABLE USE OF ICT RESOURCE POLICY

KNUST ICT resources are provided primarily to facilitate a person's work as an employee or student or other role within the University. Use for other purposes, such as personal or recreational use is a privilege, which can be withdrawn. In all cases, users are obliged to use resources responsibly to ensure their availability to other users.

Acceptable use of the University ICT resources

Acceptable use of the University ICT resources may include:

- Use for official University business.
- The use for academic and research work.
- Recreational use if it is in keeping with the framework defined in this policy, and such use does not interfere with one's duties, studies or the work of others.

Unacceptable use of the University ICT Resources

Unacceptable use of the university's ICT resources may include but are not limited to:

- Attempts to break into or damage computer systems within the network or in other connected networks.
- Attempts to access computers for which the individual is not authorised.
- Unauthorized access to another user's files.

- Attempting to circumvent Network Access Control, including by-passing proxies and firewalls.
- Monitoring or interception of network traffic without permission.
- Probing for the security weaknesses of systems by methods such as port-scanning and password cracking, without permission.
- Unauthorized extension or retransmission of network traffic including the installation of unauthorized wireless access points, routers, or switches.
- Unauthorized reselling of network and Information Management systems services.
- Unauthorized modification of university's data.
- Unauthorized download, installation or running of programs or utilities that may flood the network, causing denial of service to other users.
- Sharing of network access credentials with third parties for purposes of defeating network authentication.
- Using the network to break into other networks.
- Creation, retention, downloading or transmission of any offensive, obscene, or indecent images or data, or any data capable of being resolved into obscene or indecent images or material.
- Creation, retention, or transmission of material with the intent to cause annoyance, inconvenience, or needless anxiety.
- Intellectual property rights infringement, including copyright, trademark, patent, design, and moral rights.
- Sending electronic mail that purports to come from an individual other than the person sending the message using, for example, a forged address.

- Using the resources for unsolicited advertising or transmission of electronic mail with intent to defraud, often referred to as “spamming”.
- Deliberate unauthorized access to networked resources, local or remote.
- Deliberate activities that may result to one of the following.
  - Wasting of support staff time in support of systems
  - Corrupting or destroying other users’ data
  - Violating the privacy of other users
  - Denying services to other users
- Actions or inactions which intentionally or unintentionally, aid the distribution of computer viruses or other malicious software.
- Download, installation, and use of unlicensed software on the university network or computers.

DISPOSAL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY EQUIPMENT POLICY

Policy Statement

The University Information Technology Services Directorate is mandated with the management of disposal of all university ICT equipment in conjunction with the University's Board of Survey. The UITS in consultation with end user units, will develop guidelines and make recommendations for useful life spans of different ICT equipment, salvaging, storing, donating, trashing and disposing of obsolete information technology products.

Through the UITS Directorate, the University will maintain partnerships with relevant policy and disposal organizations like the Environment Protection Agency (EPA), electronic waste collectors, refurbishers, ICT importers and assemblers, distributors, and retailers.

All University user (academic and administrative) units are required to avail obsolete ICT equipment to the UITS for disposal in collaboration with the Board of Survey.

Procedure

The UITS, will electronically track the physical locations and status of all core ICT hardware components on the university network in its database.

Any user unit wishing to dispose of obsolete ICT equipment should contact the UITS which will evaluate the hardware and determine the appropriate course of action, according to set guidelines.

Means of Disposal of ICT Equipment

All hardware for disposal or sale should be presented to the UITS Directorate for technical inspection to ensure that it does not contain any licensed software or university information. The Systems Administrators at the user units will delete all information on the hardware and replace existing software with free equivalents before the technical inspection.

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.

WEB CONTENT PUBLISHING POLICY

Policy Statement

The University considers web publishing to be a key strategic resource for communication, teaching, research, marketing, and administration. The appropriate use of this technology by the University community is encouraged. However, the University reserves its right to define and limit the terms of use of its websites. University resources may be used to create/publish web pages where the purpose and effect of the published information is in support of the University's mission. This means that the content of web pages hosted on university resources must relate to the official activities and functions of the University or relate to the official role of members of the University community.

Web Content Publishing Requirements

Accessibility

KNUST web sites must strive to adhere to the Web Content Accessibility Guidelines of the World Wide Web Consortium. These guidelines are required of all University Web sites.

Redundancy

Do not repeat static information maintained elsewhere by the University. Instead, use data feeds, if available, such as RSS/XML, or simply link to that specific University information. Redundant information, especially different published versions, is confusing to our audience and may result in severe consequences if incorrect information is posted.

Content Validity

i. KNUST controlled sites must be registered under the knust.edu.gh domain name.

ii. Individual units at KNUST are responsible for the content on all their web pages.

iii. Content must be up-to-date and follow all sections of this policy and its supplements, as well as national laws and codes.

iv. The verbiage surrounding links to Webpages outside of the University structure cannot be written in such a form that implies endorsement, sponsorship, or other corporate gain.

v. The Director of UITS/Deputy Registrar of the University Relations Office has the right to remove the link from all University Web pages to any units that do not follow this policy or its supplements (exceptions are those units that have specific, written permission not to follow certain restrictions).

vi. No official unit may go outside the University Web structure and represent itself on another Web server or domain without written approval from the Director of UITS/Deputy Registrar of the University Relations Office.

vii. Visible credits such as "Site powered by..." or "Site created by..." are prohibited.

Copyright

i. All University Web pages should follow copyright laws.

ii. Publishers must have permission from any copyright holder to use text, photos, graphics, sounds, or movies to which KNUST does not hold copyrights.

Style

i. Official University style guidelines must be followed on all Web sites. These guidelines are outlined and detailed in the University Style Guide, which is maintained by the University Relations Office.

ii. Web-specific styles, including, but not limited to, templates, headers, footers, navigation elements, specific required tags, and other required information are outlined in the Web Standards Guide, a supplement document to this Policy, and must be always followed.

E-LEARNING POLICY

The opportunities provided by e-learning to enhance education are vast:

E-learning provides opportunities for university students to partake in virtual classes without the constraint of time, place, or distance. Unlike the traditional learning environment, video lectures can be sped up or slowed down and moved forward or backwards. Students can playback the video repeatedly and as many times as desired. All questions asked in discussion forums are always available to students. Students can ask their own questions and all others in the class can view, share answers, experiences, and their own unique perspectives. In effect, this is a better environment for some classes of learners as it provides a virtual environment to navigate every comment, question and interaction of the instructor and each student.

E-learning provides the opportunity for smaller class sizes. A blended learning environment which puts the choice of learning method in the hands of students would lead to smaller classroom sizes. Students who are good at studying on their own could opt for the online version of courses and may indeed finish ahead of their colleagues who opt for traditional instruction.

E-learning provides the opportunity for not holding back fast students and not hurrying slow students along. Self-paced learning allows both slow students and fast students to take courses at their own pace. Extremely fast or gifted students would not be held back by a slow class while slow students would not be hurried along and can take their time to repeatedly watch class videos and go through discussion forums until they have a firm grasp of the course being taught before moving on. Such online courses are time-bound but the slow student can make use of extra hours without being hurried along.

Scheduling of exams and spaces for large exams can be challenging. E-learning provides opportunities for breaking these exams up into smaller exams without compromising on quality. Techniques used to ensure quality involve the use of large question banks and shuffling of both questions and answers. This is done while ensuring that delivered question sets for exams, though different, are delivered to a similar standard or level of difficulty.

E-learning provides the opportunity for continued learning even if whole universities are physically shut down. They could still be operating, seamlessly, online.

Policy Principles

KNUST will make optimum use of technology in teaching and learning. KNUST will make use of E-learning and blended learning approaches to advance the realisation of its goals in providing learner-centred learning experiences that are flexible, responsive, and effective and meet the needs of all its learners and stakeholders. The use of synchronous and asynchronous e-learning is encouraged. The decision to use either is left to the discretion of course lecturers.

KNUST will ensure that its e-Learning provision meets the needs of a full array of flexible, independent learning experiences. Students taking e-Learning courses would have equity of opportunity with those taking courses delivered in more traditional ways. In addition, the marketing, enrollment, administrative and support procedures for such courses would be fully aligned to the needs of the e-Learner.

The University will ensure that as far as possible, resources for both tutors and learners, including e-Learning course content, University e-Resources, and those provided from external sources are easily accessed from point of need. In addition, it will, via the use of managed repositories, ensure that University owned e-Content and e-Resources are readily available and will thus actively support cross discipline and Faculty developments.

The University, through its quality processes, will ensure that e-Learning provision meets established standards expected by the University, stakeholders, relevant legislation, and that it is accessible, educationally sound, engaging and appropriate to its target populations, whilst ensuring that course developers and those facilitating learning have the freedom to innovate and apply their professional skills and judgement.

The University will promote research, scholarship, and development in all aspects of e-Learning, and in particular, pedagogy for e-Learning. It will also ensure that support and teaching staff have the requisite capacity, and clearly defined roles to ensure effective provision of e-Learning services.

The University will monitor and evaluate the use of all systems and practices contributing to its learners' e-Learning experiences, to ensure that practice, policy, and strategy are responsive to lessons learned and agile in respect of new opportunities and will actively seek to remove barriers that impede or restrict effective e-Learning.

The University will ensure that resources required to support e-Learning, in human, technical and infrastructural aspects, are appropriate to its requirements and will allow the provision to its e-Learners, realistic definitions of the levels of service they can expect.

E-RESEARCH POLICY

E-Research refers to large-scale, distributed, information-intensive forms of inquiry conducted collaboratively between institutions, and intra – and inter-nationally. The University will explore initiatives which support e-research and information management using new technologies which emphasise interoperability and flexibility.

E-Research embraces research methodologies emerging from the increasing access to distributed high-performance computing resources, data resources, research instruments and facilities utilising the Internet and local area networks and advanced communications technologies.

Policy Principles

Measures would be instituted to enable researchers from several institutions to access distributed datasets that can be integrated, searched, and queried by researchers in each institution while addressing security of data and research records, privacy, intellectual property, and ethical issues.

Build collaborative e-research environments. These include technical infrastructure, standards, interoperability, security, middleware, sharing of and access to resources between institutions and subject disciplines, licensing, user and community needs, curation, preservation, and digital rights management.

Promote the establishment of a collection of distributed computing resources (data repositories, specialised scientific equipment, computing power, knowledge services) that will enable researchers at spatially remote locations to work together collaboratively.

Ensure successful distribution of data on a national or international level by clarifying the rights and responsibilities of those who provide and use these. This will enable researchers to share data while maintaining security and confidentiality.

Establishing a clear and definitive legal position in relation to the ownership of data to enhance the opportunity for academic research and industrial innovations.

Procedures

Researchers must be permitted to protect their work, and industrial partners allowed to establish fair licensing arrangements.

Define legal structures for the ownership of intellectual property rights to clarify concerns and enforce compliance.

Prevent tensions which may arise over sharing of data by resolving at a contractual level. Research data may be licensed for use by another research group, but only on terms that ensure the resulting work will not compete with the owner's own research.

Provide the E–Security Framework for Research to establish a framework to foster collaboration and enable the secure sharing of resources and research infrastructure.

Provide Research repositories and access services for research outputs which are a key component of an institution's e-infrastructure. KNUSTs institutional repository would offer management and dissemination of digital materials created by the members of the KNUST community. This will provide an avenue for dissemination and preservation of scholarly works of students and researchers.

Establish a centre of excellence for the management of scholarly assets in digital format. Its overall focus is on the critical issues of access continuity and sustainability of digital collections within partner institutions.

Focus on sustainable standards-based management and storage of research data and raw research output.

Establishment of an e-Research Expertise Centre. This will build on existing local, national, and international expertise, tools, software, and information infrastructure to develop an integrated and cross-disciplinary model for exchanging information between research groups. The e-Research Expertise Centre will also support the national e-research community in managing and sharing research output, specifically large sets of data and information generated during research.

Establish local, national, and international partnerships and develop a suite of services and infrastructure for e-Research.

Continual improvement of the information infrastructure is critical to ensure projects are developed with new technologies and devising innovative ways of using existing technologies.

Make use of high bandwidth internet connections, data compression algorithms and fast data processing to provide a rich set of tools using video conferencing and data sharing. This enhances the ability of our researchers and students to better access data resources of all types, whatever the provenance of the data.

CLOUD STORAGE AND SECURITY POLICY

Purpose

This policy describes secure practices for Kwame Nkrumah University of Science and Technology's, faculty, staff, and students (collectively, The Institution) use of cloud software and storage services. It also highlights security risks introduced by storing non-public information (data) in the cloud and mandates the protection of data stored by Cloud Service Providers (CSPs) with appropriate technological controls.

Scope

This policy applies to all the Institution's data stored or processed by third-party cloud applications, and to all external cloud services, including cloud-based email and document storage.

Background

The Institution outsources certain technological services and data storage to third party CSPs. IT Leadership must determine what kinds of data are appropriate for storing and sharing via cloud services, and how to protect that non-public information. Data classifications can be found in the Data Classification Policy.

Policy Statement

Governance

IT leadership must approve any deployment or use of cloud-based services for storage and retrieval of Institutional systems or data. The Institution is responsible for ensuring that proper security measures are enforced for any cloud storage service offered to faculty, staff, and students. IT Security must define a process for vetting vendors of cloud platforms. This process must involve an assessment of the security posture of any vendors whose cloud platforms will be housing the Institution's data, and the acquisition of contractual terms and conditions from those vendors to take reasonable steps to maintain control and protection of the Institution's data housed on their platforms. Additionally, the University Information Technology Services (UITS) must have administrative access to all cloud applications.

Acceptable Use

All employees, faculty, staff, and students who utilize cloud services for data storage must do so in accordance with this policy and the Acceptable Use Policy. The Institution's data must only be stored in an approved third-party cloud application. Any additional cloud solutions proposed must meet the sets standards for security to qualify for consideration.

DATA CLASSIFICATION POLICY

Purpose

The purpose of this policy is to define the categorization of data assets at Kwame Nkrumah University of Science and Technology for faculty, staff and students (collectively, The Institution). This policy describes categories to which all of the Institution's non-public information types (data) should be mapped to help the institution protect data in a consistent and appropriate manner.

Scope

This policy applies to all the Institution's data. For the purposes of this policy, this includes electronic data either at rest or in transit. Additionally**,** this policy applies to any data that is hosted or accessed by third-party service providers.

Definitions

- **Personally Identifiable Information (PII):** Information which can be used to distinguish or trace the identity of an individual (e.g., name, Social Security Number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. Linked data (such as an individual's name in conjunction with their Social Security Number) can be more sensitive than an individual data point.
- **Protected Health Information (PHI):** Any individually identifiable health information transmitted or maintained in electronic media, or in any other form of medium.

- **Data Protection Act 2012:** An act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters.

Policy Statement

Data may be classified as follows:

Sensitive

Any data where the unauthorized disclosure, alteration, loss, or destruction could result in a significant harm to the Institution. Data to be classified at this tier may include, but is not limited to, PHI, PII, and any data protected by national or local laws and regulations or industry standards. Data should be classified as critical if loss of that data would:

- Cause personal or institutional financial loss or be a violation of a statute, act, or law
- Constitute a violation of confidentiality agreed to as a condition of possessing, producing, or transmitting data
- Require the Institution to self-report to the government and/or provide public notice if the data is inappropriately accessed
- Cause significant reputational harm to the Institution

Confidential

Any data where the unauthorized disclosure, alteration, loss, or destruction would have an adverse impact on the Institution's mission, safety, finances, or reputation to a lesser extent than data classified as Sensitive. Data to be classified at this tier may include, but is not limited to:

- Records disclosed to University officials with legitimate educational institutions.
- Unpublished research data

- Unpublished Institutional financial information, including strategic plans, real estate plans, or facility development plans

Internal

Any Institutional intellectual property to which employees, faculty, staff, or students may have authorized access. Internal data includes, but is not limited to:

- Internal communications, such as emails, reports, and other documents
- Research information
- Documents including manuals, technical documents such as system configurations, any standards or procedures developed to guide the Institution's decisions, or project plans that are strictly for the use of the Institution's personnel or its constituencies.

Public

Any data where the unauthorized disclosure, alteration, loss, or destruction would have little to no adverse impact on the mission, safety, finances, or reputation of the Institution. Generally, public information is classified as low risk. Publicly accessible data includes:

- The Institution's financial statements and other reports filed with government agencies available to the public.
- Copyrighted materials that are publicly available

Storage and retrieval of all data must be according to the data classification protocols and access rights outlined in this policy document.

ACCESS MANAGEMENT POLICY

Purpose

The purpose of this policy is to mandate requirements for access management controls across the technological environment at Kwame Nkrumah University of Science and Technology for faculty, staff and students, (collectively, the Institution). This policy will aid the Institution in managing access to its information systems.

Scope

This policy applies to all information systems used throughout the Institutions, whether managed centrally or in a distributed fashion. This policy applies to all individuals and entities who intend to access the Institution's information systems and data, including relevant third-party service providers and hosted/cloud-based systems.

Background

Access to the Institution's electronic information resources must be managed in a manner that maintains the confidentiality, integrity, and availability of institutional resources, and in a manner that complies with any applicable legal and regulatory requirements.

Definitions

- **Authentication:** The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Authorization:** Access privileges granted to a user, program, or process or the act of granting those privileges

- **Multi-Factor Authentication (MFA):** Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., token generation device); or (iii) something you are (e.g., biometric).
- **Least Privilege:** The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
- **Privileged Access Management (PAM):** The process of managing and protecting credentials to accounts that have some level of administrative access to devices or systems, including local administrator accounts and superusers.
- **User:** Individual or (system) process, acting on behalf of an individual, authorized to access a system
- **Organization User:** An organizational employee or an individual whom the organization deems to have equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization.
- **Non-Organization User:** A user who is not an organizational user
- **Privileged User:** A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Policy Statement

Access Management is the process of identifying, tracking, controlling, and managing user access rights to information systems. Any user who requires rights of entry or access to systems, applications, or data, must have their identity authenticated. Additionally, user access should be further restricted following the principle of Least Privilege, and in alignment with any Institution defined segregation of duties guidelines. The architecture for data retrieval should ensure at all times that data is created, read, updated or deleted securely and through the use of standardized and secure interfaces. Standardized Application Programming Interfaces (APIs) provide a means of allowing varied applications to communicate and work with each other in a secure and efficient manner.

User account provisioning must include creation of unique credentials for new users and disablement and revocation of a terminated user's access privileges upon termination.

Privileged access must only be provided to users as needed. Users with privileged user accounts must also have an organizational user account, which follows the principle of least privilege, and must use this organizational user account for their day-to-day job functions. Privileged user accounts must only be used when elevated privileges are required by the system or application.

Where there is any requirement for shared usage of an account this must be signed off by the IT Security division and all usage must be audited and traceable to an individual authorized user account.

All remote access to the Institution's network must utilize a secure solution, which employs multi-factor authentication, and a secure network encryption protocol.

Multi-Factor Authentication

All systems should as much as possible make use of multi-factor authentication. All systems that support multi-factor authentication should have this feature turned on.

DATA GOVERNANCE POLICY

Purpose

In order to serve Kwame Nkrumah University of Science and Technology's core purposes of teaching, research, and service, university data are held as institutional assets that are appropriately maintained and safeguarded. The term "university data" describes groups of data items relevant to the management, planning, or operations of any Kwame Nkrumah University of Science and Technology unit, or information that is used or reported in legally binding administrative University reports.

University data must be easily integrated throughout the University's information systems and must accurately represent the information intended and promote effective and innovative administration. For Kwame Nkrumah University of Science and Technology's administrative data systems, particularly the student, financial, and human resource systems, data governance aims to create university-wide policies and procedures that guarantee university data satisfies these requirements. It seeks to define the vision for data governance in the university and ensure that data are managed consistently and used properly.

Scope

This policy applies to all data used throughout the University, whether managed centrally or in a distributed fashion. This policy applies to all individuals and entities who access the University's data, including relevant third-party service providers and hosted/cloud-based systems.

Background

Data governance as a principle includes directives across people, processes, and technologies. Data governance policy entails the following:

- **data governance structure** – identifying the roles and responsibilities of individuals and groups who have been identified as key players in the management of data
- **data access policy** – a policy for enabling rightful employee and third-party access to data assets (refer to "access management policy")
- **data integrity and integration policy –** this ensures that business units have access to data they can rely on. Data must be integrated across sources, systems, applications, and tools without compromising integrity, and lastly
- **data usage policy** – this ensures the ethical usage of data. The ethical usage of personally identifiable information (PII) is more important than ever before with the advent of regulations such as the General Data Protection Regulation (GDPR). (refer to "data classification policy")

The University's data must be managed in a manner that maintains its confidentiality, integrity, and availability. Furthermore, the management processes must comply with any applicable legal and regulatory requirements.

Definitions

- **Personally Identifiable Information (PII):** Information which can be used to distinguish or trace the identity of an individual (e.g., name, Social Security Number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. Linked data (such as an individual's name in conjunction with their Social Security Number) can be more sensitive than an individual data point.

- **GDPR**: General Data Protection Regulation
- **Control-centric data governance**: In a control-centric data governance model, one person is usually designated as the data governance lead, responsible for making decisions and providing direction for the program. In some organizations, that person may also be accountable for managing master data and distributing it to users as needed or upon request.
- **Data Governance Group**: the body that will oversee the proper governance of data in the university.

Policy Statement

Data Governance Structure

Data governance is the process of ensuring data quality, stewardship, protection, compliance and proper management. It presupposes a philosophy of open access to university data by all community members together with the obligation to abide by all rules and regulatory restrictions that regulate that use. In the interest of attaining effective data governance, Kwame Nkrumah University of Science and Technology adopts a control-centric approach to data governance and assigns staff to implement them. While the University Data Administrator is assigned a leadership role with oversight for the activities of data governance, this function is shared among the executive sponsors, data stewards, data custodians, and data users.

Overview of University Data Governance Roles

The major tasks and responsibilities within Data Governance are as follows:

Aspect: Director, UITS

Definition: Appoints the other data governance players and has planning and policy responsibility and accountability for major administrative data systems (e.g., student, human resources, and financial) within their functional areas.

Key Responsibilities:

1. By understanding the planning needs of the institution, the Director, UITS must anticipate how data will be used to meet institutional needs and offer direction.
2. Serves as the final escalation point for resolving all data-related conflicts

Aspect: Data Administrator/Manager (Deputy Director, Software Development Division)

Definition: Oversees the implementation of the entire data governance program

Key Responsibilities:

1. Processes and transforms data for modeling while ensuring its integrity and usability
2. Serves as the first escalation point for resolving all data-related conflicts
3. Enable data analytics for decision-making: This involves handling all training and onboarding requirements for technical and business users.
4. Responsible for database administration tasks, such as maintaining the data dictionary, and monitoring database performance

Aspect: Data Steward (Deputy Director, Information Security & Technology Assurance Division)

Definition: Acts as a bridge between business and IT so that business users can access the right data

Key Responsibilities:

1. Helps standardize data definitions, rules, and descriptions.

2. Helps define access policies and optimize data-related workflows and communication.
3. Protecting the data assets: Responsible for establishing data security protocols that align with the university's data governance goals, policies, standards, and compliance requirements. They also assess potential threats to data security.

Aspect: Data Custodian (Deputy Director, Systems and Data Management Division)

Definition: Deals with the movement, security, storage, and use of data

Key Responsibilities:

1. Oversees data access and storage
2. Identifies data stewards for various data domains and collaborates with them on data quality issues
3. Overseeing data storage: Responsible for handling the technical aspects of data storage, versioning master data, and setting up system backups and a disaster recovery plan.
4. Controlling data access: Responsible for authorizing and controlling access to data. Responsible for managing the technical aspects of setting up and implementing permission controls.
5. Ensures proper performance of database software and hardware.

Data Access

The data access policy guarantees that staff have adequate access to institutional data and information. While acknowledging the University's duty to ensure data security, the measures put in place to do so must not unreasonably impede the effective operation of university operations. Regardless of the offices or formats in which the data are stored, this policy is applicable to all University units and all uses of institutional data.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, and unnecessary restrictions on its access. The University will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant data steward to have an appropriate access level. Data access will be conducted in accordance with the policies established by the University Information Technology Services (UITS).

Any employee or non-employee denied access may appeal the denial to the Data Governance Group or Executive Sponsors.

Data Usage

The data usage policy aims to prevent exploitation and abuse of university data and to guarantee that it is used responsibly, in compliance with all applicable laws, and with proper regard for personal privacy. The security levels defined/given by the data steward and implemented by the data custodian determine how the data is used.

Employees of the university shall only access and use data as necessary for the fulfillment of their duties, and not for selfish or other improper reasons. They must also access and use data in accordance with the security levels allocated to the data.

Only employees whose job responsibilities specifically and mandatorily include responsibility for data update shall be given authority to update data by the authorized data steward. This constraint should be balanced with the university's goal to offer top-notch services to faculty, staff, students, and other constituencies rather than as a mandate to restrict update authority to members of any one group or office. Employees will be given the minimum access required to administrative data required for them to do their work effectively. For official or non-official reporting, data pieces may be externally distributed according to the Data classification policy and any other relevant policy or document. The requirement to maintain data integrity and respect individual privacy should guide the dissemination of information. The data steward must give consent before releasing any such data. University

Information Technology Services (UITS) has set policies that must be followed while using data.

The consequence of non-compliance with the Data Usage Policy of the University by employees and students will be considered a violation of the relevant University codes of conduct and may be subject to disciplinary action or to legal action if laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data.

Data Integrity and Integration

In order for university academics, staff, and management to rely on data for information and decision support, this policy aims to ensure that University data have a high degree of integrity and that important data pieces can be integrated across functional units and electronic systems.

Data validity, reliability, and precision are all referred to as having "data integrity." The consistency of each data element's definition and a thorough understanding of the business processes that underlie the data are prerequisites for maintaining data integrity.

Data integrity and the creation of a data model, associated data structures, and domains are prerequisites for data integration, or the capacity of data to be absorbed across information systems.

University data will be uniformly interpreted across all university systems in accordance with the best practices decided upon by the Data Governance Group. Data administration will make sure that the requirements of data users are taken into account when developing and changing data structures, domains, and values. Each data steward is accountable for making sure the data values for the elements under their charge are accurate.

University data are defined as data that are maintained in support of a functional unit's operations. It is the responsibility of each data steward, in conjunction with the Data Governance Group, to determine which core data elements are part of university data. Documentation (metadata) on each data element will be maintained within a university repository according to specifications provided by the Deputy Director of, Software Development Division and informed by the Data Governance Group. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic calendar. All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards, the Data Governance Group, or the Deputy Director of, Software Development Division.

REFERENCED POLICIES

https://www.sgu.edu/office-of-information-technology/computing-policies/cloud-security/

https://www.sgu.edu/office-of-information-technology/computing-policies/data-classification/

https://www.sgu.edu/office-of-information-technology/computing-policies/access-management/

https://it.tufts.edu/about/policies-and-guidelines/cloud-computing-services-policy/

www.unlv.edu/sites/default/files/page_files/27/Policies-DataPolicy.pdf

https://atlan.com/data-governance-roles-and-responsibilities/

https://policies.mak.ac.ug/sites/default/files/policies/Acceptable_Use_of_ICT_Resources.pdf

https://fdocuments.in/document/makerere-university-ict-policy-master-plan-2010-2014-1.html

Quality Assurance and Planning Office
Vice-Chancellor's Office
Kwame Nkrumah University of Science and Technology
KNUST, Kumasi
PMB UPO, Kumasi-Ghana
Tel: +233 322060319
Email: info.qapo@knust.edu.gh

ISBN: 978-9988-2-8487-9

9 789988 284879