wjert, 2021, Vol. 7, Issue 5, 16-26. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org SJIF Impact Factor: 5.924

TAMALE TECHNICAL UNIVERSITY DIRECTORATE OF ICT SERVICES

Mohammed Mahfouz Alhassan*[1], Mohammed Nurudeen Alhassan[2], Adam Wahab Legma[3]

[1]Head, ICT Strategy and Plan Implementation, Assistant System Analyst, Directorate of ICT Services, Tamale Technical University.

[2,3]Junior Assistant ICT Officer, Directorate of ICT Services, Tamale Technical University.

Article Received on 28/06/2021 **Article Revised on 18/07/2021** **Article Accepted on 08/08/2021**

***Corresponding Author**
Mohammed Mahfouz Alhassan
Head, ICT Strategy and Plan Implementation, Assistant System Analyst, Directorate of ICT Services, Tamale Technical University.

ICT POLICY

(Information Communication Technology Policy)

NITA-National Information Technology Association

CMG - Change Management Group*

CD - Compact Disk

DVD - Digital Video Disk

ICT - Information & Communication Technology

ICTCC - ICT Council Committee

IICTIC - ICT Implementation Committee

ICTSC - ICT Steering Committee

IRM - Information Resource Management

ISP - Internet Service Provider

KENET - Kenya Education Network

LAN - Local Area Network

Mbps - Mega bits per second

MIS - Management Information System

SMTP - Simple Mail Transfer Protocol

STEP - Skills Training for End-users Project

TCP/IP - Transport Control Protocol/Internet Protocol

UPS - Uninterrupted Power Supply

VSAT - Very Small Aperture Satellite

WAN - Wide Area Network.

Tamale Technical University ICT Policy

The Tamale Technical University ICT policy provides comprehensive principles and procedures to ensure all students and staffs is made known of their responsibilities and obligations when using ICT equipments and resources at the University. Any Access to all or some of the ICT facilities and resources are a privilege and not a right. Inappropriate use will involve corrective action and could result in confiscation of equipment, exclusion from accessing ICT resources and equipment and police investigation which may be out of the control of the Tamale Technical University.

INTRODUCTION

The Tamale Technical University provides a wide-ranging range of information and communication technology equipments, resources and services to all students and staffs.

The University Board and Leadership Team are expected to ensure responsible use of Information and Communication Technologies (ICTs) by all students and staffs both on and off campus. This includes the use of all computing hardware, software, email, the Internet, Intranet, social networking sites and Tamale Technical University information systems.

It also includes the use of any Bring Your Own Device (BYOD) personal equipments, including laptops, tablets, USBs, mobile phones, MP3 players and cameras. Students and staff are advised not to violate any laws, regulations, or Tamale Technical University policies or procedures, including:

- The Tamale Technical University Privacy Policy
- Tamale Technical University Behavior Policy
- Tamale Technical University Cyber Safety Policy
- Tamale Technical University Copyright Policy
- Tamale Technical University BYOD Code of Conduct (BYOD) Bring Your Own Device

Tamale Technical University advices all students and Staffs also that the Tamale Technical University would not accept responsibility for the loss, damage or theft of any personal property belonging to staff or students.

Legal and Ethical Responsibilities

Students and staff need to know that it is unlawful to use mobile phones or electronic devices to

- Threaten others or incite violence.
- Post pictures of other students on websites or social networking sites without the formal, written consent of the parents of such students.
- Torment or harass other students.

Any incidents may result in the device being confiscated and the incident being reported to the police.

No abusive emails, pictures or information are to be sent or received by staff and students. Please notify your teacher or the ICT Manager immediately if you receive any offensive electronic communication.

ICT Policy Review

The Information Communication Committee (ICT) will review this policy (5) years and report to the Vice Chancellor or Pro-Vice Chancellor with any new statutory requirements or recommendations for amendment.

Special category personal data

Special category personal data is a subcategory of personal date. The special category personal data requires additional protection.

Special category data is any personal data that relates to a person or persons:

- Race;
- Ethnic origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;

ICT Policy Approved By.

SIGNED		
SIGNED		
SIGNED		
SIGNED		
SIGNED		
SIGNED		

Student Privacy Policy

Each and every student will have an e-learning account created when they join Tamale Technical University.

They will be enrolled in the courses they are pursuing for the semester and Will have access to the courses.

Every student will have access to their particular account and be advised to

Set up a very strong password involving both letters and numbers and some special characters.

Each and every Lecturer's supposed to ensure they grade the assignment`s that they give and the marks will only be detectable to the particular student, thus ensuring student's privacy.

ICT Education policies

The use of ICT in education is so clear in many regards, same are the 'perils' related to the distraction of existing conventional teaching and learning practices, soaring costs, increases burdens on teachers, equity and issues around data privacy and security.

Policies related to ICT technology use in the change that evolve over time, most often along a somewhat predicable alleyway, and sometimes technological innovations are often outpace the ability of policymakers to innovate on some related policy issues. Such policies take different forms/norms and are formulated and proposed by sometimes different institutions in different countries. No matter the country, a lack of meticulous, relevant evidence typically complicates attempts to draft impactful ICT/education policies.

As part of the work under the World Bank's Systems Assessment for Better Education Results (SABER) initiative, the World Bank is attempting to document some national educational technology policies around the world and their evolution over time.

A related SABER-ICT policy framework has been developed to assist policymakers as some of them they attempted to analyze and standard their own policies on ICT use in educational sectors world over against international norms and those of comparative countries around the world, identifying some key themes and characteristics, drawing on an analysis of a related policy documents.

Some Eight policy themes are commonly acknowledged in educational technology policies around the world. These relate to (1) ideas and plans; (2) ICT infrastructure; (3) teachers; (4) skills and competencies; (5) learning resources; (6) EMIS; (7) monitoring and evaluation; and (8) equity, inclusion, and safety. Four stages of policy development can be identified interconnected to each of these themes.

It is important to note that this framework only considers policy intent – not the extent to which policies are sometimes implemented in practice, what the impact of such policies may be, and that rapid developments and innovations in the technology sector challenge the abilities of policymakers to offer some useful related policy guidance that is forward-looking.

Policymakers may find the SABER-ICT policy framework useful as a means by which to help benchmark the current state of related policy developments in their country; and anticipate potential future policy directions; and draw inspiration from other countries.

Data Security Policy

Management and Staff and guardians of administrative data are expected to manage, the access, and utilization of Tamale Technical University data in a manner that maintains and protects the security and confidentiality of the Tamale Technical University information. Any notice of State & local regulations must be considered and adhered to when using or sharing of personal or confidential information. Any notice of a breach of confidential information whether in paper or electronic form MUST be reported to the Tamale Technical University Security Officer immediately.

Personal Digital Assistant Policy

Tamale Technical University encourages the ownership and use of personal electronic devices it does not provide hands on support for legal reasons. The PDA policy define standards, procedures, and restrictions for the use and support of Personal Digital Assistant

devices (PDAs) that are commonly used in the workplace and may be used by employees of Tamale Technical University and it's students.

Technology Renewal Policy

Tamale Technical University strives to keep up a sustainable technology infrastructure that will support the learning environment and to enable efficient business practices.

Wireless Network Policy

Tamale Technical University provides wireless networking services in public spaces on campus to enable the convenience of mobile network connectivity.

This service allows staff of Tamale Technical University to access the campus wide network from wireless devices or portable computers where coverage is available on Campus.

Electronic Communication (email) Policy

Tamale Technical University provides access to email and the University's portal for all students, faculty and staff. Email is one of the official methods of communication at.

Tamale Technical University. Students and staff are held strictly responsible for the consequences of not reading University related communications sent.

To their official email Tamale Technical University dress. Tamale Technical University. students will also utilize the University`s portal.

Related announcements. The purpose of this policy is to identify electronic communication as an official means of communication within Tamale Technical University. And to define the responsibilities of Tamale Technical University. Students, faculty and staff related to electronic communication.

Tamale Technical University reserve the right to monitor the use of our ICT services, and access to any information stored on Tamale Technical University ICT infrastructure, but, Tamale Technical University will do so in ways that are consistent with the relevant legislation and guidance the Information, Tamale Technical University will undertake such actions to:

- Comply with our regulatory and statutory obligations.
- Assess compliance with our Information Security and Acceptable Use Policy

- Maintain effective ICT systems
- Prevent and detect unauthorized use or other threats to our ICT systems
- Monitor system performance.

Such monitoring may include email, internet, telephone, mobile telephone and electronic file storage usage. Such monitoring is not, in general, person specific; however, it may be unavoidable personal data may be accessed as part of this policy.

Tamale Technical University shall make users aware of this policy by:

- Highlighting the policy in the staff privacy notice.
- Ensuring all members of staff is informed of the policy at their induction.
- Informing staff of the terms of this policy by logging onto Tamale Technical University ICT infrastructure.
- Reminding users at regular intervals, e.g. at the point of log on, of the existence of the policy and any updates to it, and where to find it.

Privacy

Tamale Technical University policy aims to provide an appropriate balance between respecting your privacy and allowing the necessary monitoring required meeting our business needs and legal obligations.

We recognize that staffs of Tamale Technical University have legitimate expectations that they should be able to keep their personal lives private and that they are entitled to a degree of privacy in the work environment.

The use of a firewall to secure your internet connection. This creates a safety barrier between your network and the outside world.

- **Selecting the most secure settings for your devices and software**.
- Most often the default settings for software and devices are pre-configured to be as open as possible. It is important to re-configure these to make them secure, including the use of two factor authentication where appropriate.
- **Restrict access to data and services.** It is important to ensure that staffs have appropriate access and to review user access on a regular basis.

- **Protect data with appropriate anti-virus and anti-malware.** It is essential to install appropriate anti-virus software along with anti-malware software to reduce external threats and to ensure that definitions are updated regularly.
- **Keep your software and devices up to date.** This can be achieved using patch management software which ensures all security patches are applied accordingly.

To achieve Cyber Essentials, certification involves a self-assessment questionnaire and an external independent vulnerability scan. The above recommendations are already in practice within.

Tamale Technical University is aiming to achieve Cyber Essentials Plus certification by the end of 2025 which involves an additional internal scan and on-site assessment.

Information security principles

We will ensure that we manage effectively

- The integrity of our information to ensure its completeness and accuracy.
- The confidentiality of personal or sensitive information.
- The prevention of unauthorized access to, use or disclosure of our information.
- Business continuity by protecting our information from internal and external security incidents.
- The physical security of our information.

Records Management lifecycle

We will manage our records throughout the full lifecycle: from the creation or receipt of information, through to managing its use, maintaining its integrity, controlling its storage and retrieval, to its final transfer or disposal.

Our records management relies on.

Procedures

The safety and wellbeing of all staff and students at Tamale Technical University is the joint responsibility of all families and staff. It is essential that families work closely with the College staff to ensure that all ICTs are used responsibly at all times.

Specific procedures are outlined below to protect the rights of individuals to privacy and also to ensure that students and staff do not act unlawfully, nor cause harm to others.

Protect the Safety and Wellbeing of all Staff and Students

We are all responsible for ensuring that Tamale Technical University provides a safe, supportive learning environment for all students and staff. This means that:

1. Abusive, threatening or hurtful emails, posts, messages, pictures or behaviors will not be tolerated and will result in immediate corrective action. The police will be notified at the management discretion.
2. Disrupting others' learning or damaging others' property will result in restorative justice whereby the cost of replacing the property and/or repairing the damage will be borne by the perpetrator.
3. Disrupting learning through accessing inappropriate content or listening to loud music will result in confiscation of the relevant device.
4. The sending of any messages without clearly identifying the sender's details is in breach of this ICT policy and will result in the immediate suspension of ICT privileges and access.

Uphold Laws regarding Copyright and Intellectual Property

- It is illegal to copy any software, graphics, text, games or music that may contravene copyright laws.
- Copying files, passwords or work belonging to another person may be deemed plagiarism and/or theft.
- Never bring 'pirate' copies of films, games or other multi-media to school or share them with friends using school equipment or resources.
- All files and materials created using Tamale Technical University equipment and resources are deemed to be the property of the Tamale Technical University. This includes the access of University`s information and resources from outside the school.

Safeguard Security Data and Information

- Never reveal your password to another person. Change your password regularly and be aware of others watching you enter your password to log-on.
- If you share your password with others and they use it inappropriately you will be held responsible.
- Respect all security provisions on the computer network.
- Do not share personal information or inappropriate materials with others via the College network.

Remember that all electronic information sharing cannot be guaranteed to be private. The ICT Management may review, delete or recover files or directories at any time. Students can also expect teachers to have access to read student files in particular instances.

Use Online Resources Appropriately

1. Do not advertise, sell or promote any illegal products or services via the University computing and information systems.
2. Make sure that you never send, share, view or access offensive or inappropriate websites, apps, files or emails. only subscribe to authorized and approved discussion lists, chats or news groups.
3. Do not download and/or install non-approved files, programs, apps, plug-ins or other software. Contact the ICT Department for permission to use non standard software or support features.

Consequences for inappropriate use of ICT systems and devices at Tamale Technical University

Violations of this policy may result in immediate suspension of access to all ICT resources and facilities. In case of criminal negligence, the police will be notified and disciplinary action may be taken by the management or by relevant state authorities which may be out of the control of the school.

Repeat offences or inappropriate use of BYOD technologies, mobile devices and other ICTs may result in students being banned from bringing these personal items to school.

Standard procedure for student misuse of ICTs

Minor offences

- Teacher reminds student of the ICT policy and procedures.
- Student complies immediately – no further action.

OR

Student continues to ignore the ICT policy – teacher confiscates equipment or withdraws student's access privileges. Student and/or parent called to meet with teacher to determine corrective action. Student complies with policy and equipment and access rights are restored.

OR

Student continues to behave inappropriately – Head of School is notified. Student has to negotiate a gradual re-instatement of privileges.

Serious offences

- Serious offences include serious threats, or bullying, sharing of illegal or indecent information and images, or R rated content.
- The Vice Chancellor and parents will be notified and police may be called to investigate the allegation. Access to ICT equipment and resources will be withdrawn until the investigation is completed.

REFERENCES

1. Scottish Funding Council Data Protection Policy.
2. Tenison woods college, ict policy.
3. Hekima University College ICT POLICY,A Constituent College of the Catholic University of Eastern Africa, 2019.
4. ICT & education policie,Understanding PovertyEducation and Technology.The world bank.en/understanding povertyen/topic/edutech.
5. IT Security and Policies COVID-19 UPDATES The Boston Campus protocols have been updated, IT Security and Policies, UPDATED JUNE 30, 2021.