ICT POLICY
JUNE 2019

INTERNATIONAL MEDICAL AND TECHNOLOGICAL UNIVERSITY

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

ICT POLICY 2019-2023

JUNE 2019

TABLE OF CONTENTS

ACRONYMS

IMTU	International Medical and Technological University
ICT	Information and Communication Technology
LAN	Local Area Network
IT	Information Technology
TCRA	Tanzania Communications Regulatory Authority

DEFINITION OF KEY TERMS

Internet is the term for the global computer network used to share information along multiple channels, and over multiple protocols.

Device is any computer or electronic instrument capable of accessing, storing and communicating data.

Copyright is a form of intellectual property which gives the creator of original work exclusive rights in

IP address is a set of protocols developed to allow cooperating computers to share resources across a network.

Account is a combination of a username (identifier) and password allocated by an ICT Officer to an Authorized User (the account owner) to access ICT Services, Facilities and Infrastructure.

Authorized User is an individual who has been granted access to University ICT Services under one or more of the following categories:

- A current member of the governing body of the University;
- A currently employed officer or employee of the University;
- A currently-enrolled student of the University;
- Any person granted access to use IMTU ICT Services including, but not limited to:
- A contractor undertaking work for the University under the provisions of a legal contract;
- A member of a collaborative venture in which the University is a partner; or
- A visiting lecturer, student or other associate who is undertaking similar activities in a recognized University, as a registered associate

ICT Infrastructure is all electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARNet and the internet.

Software is a collection of various kinds of programs that are used to operate computers and related devices.

FOREWORD

Information and Communication Technologies laboratory (ICT) is a very important source of information for any institution of learning including schools, colleges, and universities. Being a very powerful source of information, ICT is needed by learners at different levels of acquiring knowledge and skills. Similarly teaching staff and trainers in different situations also need ICT as a source of information in order to update their knowledge. It is important to mention here that many trained professionals like engineers, medical doctors, pharmacists quite often need to update their knowledge using ICT. This will depend on the laboratory itself being up to date.

This policy includes rules for using the ICT and instructions on recovery of lost resources by students and staff. It is my hope that all IMTU community will collaborate with ICT staff to preserve its integrity. It is here for all of us to use.

Prof Kagoma S. Mnyika MD, MSc, PhD
Vice Chancellor

CHAPTER ONE - INTRODUCTION

1.1 Background Information

Information and Communication Technologies (ICT) encompass a diverse set of tools, systems, applications and services used for production, processing, storage, transmission, presentation and retrieval of information by electronic means. ICT comprised a wide range of rapidly-evolving and increasingly-converging technologies including hardware, software, networks, audio-visual systems and associated applications. The capacity of ICT is growing exponentially, whereby computers and other devices become increasingly powerful; transmission capacity increases; and software applications make it easier to create multimedia resources.

ICT has increasingly become an integral part of today's educational system throughout the world. This is mainly because information and communication are at the very heart of any educational system. ICT has the potential to support many educational functions, such as teaching and learning, research and scholarship and management and administration. These technologies enhance the sharing of information; increase collaboration among students, academicians and administrators; enhance provision of distance education; and have resulted in new forms of pedagogy. In higher education, ICT has been broken into 4 broad categories: 1) subjects (e.g. computer studies); 2) tools to support other subjects (e.g. computer-based learning); 3) educational management tools (e.g. student information systems); and 4) platforms for information sharing. Hence, the transformation of higher education must be coupled with the effective application of ICT in teaching, learning, research, outreach and administration. In order to respond to these demands, higher education institutions need to realign their practices to information age standards by adopting ICT as important tools for enhancing efficiency and effectiveness.

In view of the wide range of converging activities, the danger of the digital divides. This Policy sets out guidelines on the use of ICT systems and the consequences for non-compliance.

The Policy applies to all the IMTU University employees, contractors, consultants, agents, students and any other person who use or have access to email or files, software applications and the Internet during the course of their employment or business dealings with the IMTU University, whether such use takes place on the IMTU premises or elsewhere.

1.2 International Medical and Technological University: Overview

The International Medical and Technological University (IMTU) is a privately owned higher education institution operating in Tanzania. The owner of the University is Shri. Katuri Subba Rao, the founder of the Vignan Education Foundation (VEF).The VEF of Bangalore, India initiated the establishment of the university at the behest of the Late Mwalimu Julius K Nyerere, the Father of the Tanzania nation. The seeds of the venture were sown by His Excellency Dr. Benjamin W. Mkapa, the third President of the United Republic of Tanzania when he was the Honorable Minister of Foreign Affairs and International Cooperation. The establishment of the university symbolizes the long standing partnership between Tanzania and India as part of implementation of the south-south cooperation. The university commenced by establishing the College of Medicine which was inaugurated on 17th September 1997 by then Honorable Prime Minister of India, Shri I.K Gujral. The University is committed to provide quality higher education and its mission is therefore, to: '*Advance, expand, transmit, enhance and perceive knowledge for the people of Tanzania and the world in general.*

The vision of the University is*; 'to be a center of excellence in advancement, expansion and transmission of knowledge through training and research, outreach and public services*

The mission of the University is to: '*Advance, expand, transmit, enhance and perceive knowledge for the benefit of the people of Tanzania and the world in general'*.

CHAPTER TWO

POLICY OBJECTIVES, SCOPE, VISION AND MISSION

2.0. Main Objective

The purpose of this document is to ensure the appropriate use of the University's Information and Communication Technology (ICT) Services and define the responsibilities of users of the University's ICT Services and Infrastructure.

2.1 Specific Objectives

- Ensure Access to, and sustainable use of ICT Services
- To ensure security of data and ICT services all the time
- To develop guidelines on ICT acquisition and management.
- Improve and maintain reliable ICT infrastructure
- Develop, acquire, manage and promote utilization of electronic information resources to support teaching, learning and research activities

2.3 Scope

The ICT policy applies to all students, academic and non-academic staff of IMTU as well as outside persons and institutions who make use of ICT Services.

2.4 Vision

To be leading ICT center and provide world class ICT services.

2.5 Mission

To fully incorporate ICT into training, research and delivery of services.

CHAPTER THREE - POLICY PROVISIONS

ICT provide support to the University including research, teaching and learning, and operational activities. The conditions of use defined in this Policy, and associated ICT Policies and Procedures apply to all University members. All ICT Services provided by the University, all Facilities and Infrastructure owned by the University and to any privately owned Device that connects to University Infrastructure.

3.1 Policy Statements

In order to ensure focused implementation of ICT policy the following articles of policy statements are hereby declared:

a) Assure availability of all anticipated ICT services/systems at all workplace in the College;

b) Acquire and maintain sufficient computers to meet the needs of the staff and student population

c) Assure availability and controlled usage and changes of basic User-level Data Communication and telecommunication Services such as e-mail, Access-to-Internet/Extranet/Intranet services and telecommunication terminal equipment which actually are major 'elements' of the low-level network & communication Services;

d) Promote office computing in all offices. This applies to lecturers, researchers, administrators, managers, as well as to secretarial and clerical workers. Major office computing applications are: office packages, electronic e-mail, data and document storage and retrieval desktop publishing, access-to Internet and intranet;

e) Continuously improve both the efficiency and effectiveness of library operations and services through the implementation of an integrated on-line library information system;

f) Enhance and streamline education related administrative and managerial processes and to improve academic reporting through the implementation of an integrated academic records information management system;

g) Enhance and streamline financial management processes and reporting through the implementation of an integrated financial information management system;

h) Enhance and streamline the human resource management and administrative processes through the implementation of a human resource information system;

i) Enhance and streamline the property and asset management and administrative processes through the implementation of an asset and inventory information system;

i) Ensure availability of adequate and skilled ICT staff in terms of technical, academic and administrative staff.

j) Ensure sustainable management of the institution's ICT resources through creation of appropriate policy guidelines and regulations, advisory and operational organs that will cater for the broad interests of all users;

3.2 Access to ICT Facilities

Access to the Internet, and services provided via the Internet, are available to Authorized Users only. Access to ICT Services and Facilities may be granted to:

1) All staff and registered students and
2) Selected categories of external members

a) **Staff**

Concerns with all permanent, temporary and contract employees of the IMTU.

b) **Students**

Preferred to full-time and part-time students registered at the University in a particular year.

c) **External Members**

External members include but are not restricted to;

d) **Members of Council**
This applies to all members of Council of the University.

e) **Guest Lecturers, Research Staff, Post-Doctoral Fellows, Honorary Chairs and Professors Emeritus**
Lecturers or research staff who are not permanent staff members of IMTU, but who deliver lectures on invitation, or hold doctoral fellowships, honorary chairs or are appointed as Professors Emeritus at the University.

f) **Honorary Members**
Individuals who have been previously employed staff members of the University and on whom honorary membership has been conferred at the discretion of the Executive Director:

g) **Exchange Students**
Treated as parts of an exchange program

3.2.1 Accessing the Internet and Online Services

Use of the Internet and associated services are provided under the conditions of appropriate and ethical use. Users of this service must respect the rights of other authorized users to ensure that all have equitable privileges, privacy and protection from interference or harassment.

Internet usage must be legal and comply with the requirements of Tanzania Communications Regulatory Authority (TCRA), University Rules, Policies, and Procedures.

3.2.2 System Integrity and Support

Users shall not be allowed to disconnect PCs or other ICT equipment, from the main supply or from network connection points; doing so may corrupt data stored on the system or the current work of other users. Always the user shall contact ICT support if there is a need to move any piece of ICT equipment for any reason whatsoever

3.2.3 Appropriate Use

IMTU ICT Services must be used in an appropriate manner.
Appropriate use is considered to be the use of equipment in:

• A legal manner, meeting the requirements of legislation and University By-laws, Ordinances and Policy; and meeting the principles of fair use.

3.2.4 Authorized Users

ICT Services and Facilities are only available for use by Authorized Users. This is an individual who has a legitimate relationship with IMTU as defined in the ICT Access Control Policy.

All Authorized Users are bound by the ICT Services and Facilities Use Policy.

Associate members and other occasional users who are not Staff or Students of IMTU must sign and return a copy of the IMTU ICT Services and Facilities Use Agreement. The ICT Services and Facilities Use Agreement must be signed and returned to IT Services in order for any Associate member to be granted Authorized User status.

The IMTU ICT Services and Facilities Use Agreement may be superseded by a usage Agreement, employed by a Division, Faculty, School, Centre, Institute or Section, that has been authorized by a Senior Officer.

Where such an Agreement exists, and it meets the requirements of the IMTU ICT Services and Facilities Use Agreement and extends upon those requirements, that Agreement is binding for the Facilities to which it applies and is considered an extension of IMTU ICT Security Framework.

3.2.5 Responsibilities of Authorized Users

IMTU ICT Services must be used in a manner which supports the good name of the University and may only be used:

- In support of teaching, learning, research, personal or professional development, business operations and management or other activities officially directed towards the mission of the University; and for limited personal use.

All Authorized Users of University ICT Services must respect the rights of other Authorized Users to ensure that all have equitable privileges, privacy and protection from interference or harassment.

3.3 Internet and Online Services Access Restrictions

IMTU reserves the right to block access to internet services, or websites, where accessing, or obtaining content from, those services or websites using IMTU ICT Services, Facilities, or Infrastructure would be considered a breach of Federal or State legislation, or a breach of IMTU Policy.

IMTU reserves the right to block access to any online service which is identified as a platform for the distribution of viruses, malware, other malicious software, or is associated with solicitation of personal or financial information.

The University will make attempts to ensure any internet service, or website, which is blocked, is not used for research, teaching and learning, or University business reasons.

All access restrictions will be approved by the head of ICT department. Also the reviews of access restrictions will be heard by the Head of ICT department.

3.4 Copyright Provisions

IMTU expressly forbids the use of any of its ICT Services, Facilities and Infrastructure for any purpose which would breach copyright in any way.

The University considers copyrighted materials to include, but not be limited to:

i. Music;
ii. Movies;
iii. Television programs;
iv. Electronic publications; o EBooks; o Electronic journal papers;
v. Computer software;
vi. Unlicensed data, including unlicensed research data.

3.5. IMTUICT Services, Facilities, and Infrastructure Provisions in Relation to Copyright

3.5.1Protected Material

IMTU ICT Services, Facilities, and Infrastructure may not be used to download, copy, compress, store, transfer or redistribute content without the express permission of the copyright owner.

The University reserves the right to remove any alleged infringing material from any of its ICT Services, Facilities, and Infrastructure without prior notification.

Where a service or website, external to the University, is identified as a source of infringing material the University reserves the right to block access to that service or website.

3.5.2 Responsibilities of IMTU University Members in Relation to Copyright Protected Material

Members of the University are prohibited from using any University ICT Services, Facilities or Infrastructure to acquire, store or share materials that infringe the rights of the copyright holder.

Members may, on occasion, purchase materials via online distributors using University ICT Services, Facilities and Infrastructure. These materials may be stored on University Facilities in accordance with the license conditions under which they were purchased.

It is the responsibility of IMTU Members to ensure that, they manage their copyrighted materials in accordance with legislative and policy requirements.

3.5.3 Dealings in Copyright Protected Material for Teaching or Research

The University holds licenses which allow certain copyrighted material, including text, images, music and recorded broadcasts, to be copied, stored and communicated for the educational purposes of the University. Staff and students are obliged to abide by the license conditions for the use of this material.

The University has made available information regarding the use of copyrighted materials for teaching or research purposes at the following location on the University's web site:

• http://www.imtu.edu./copyright/

Further information regarding the use of copyrighted material for educational purposes may be sought from the ICT Officer.

3.5.4 Notices of Copyright Infringement

IMTU University makes all attempts to ensure copyrighted materials are used within licensee conditions, and that ICT Services and Facilities are not used to facilitate copyright breach.

All materials, including non-infringing materials and ICT equipment are subject to removal from the IMTU network in the event that a notice of copyright infringement is delivered against the University.

Should the University receive a notice of copyright infringement the University reserves the right to remove the material in question, or make it unavailable by disconnecting the underlying ICT Infrastructure via logical or physical action, until such time that a determination about the legitimacy of the infringement claim can be made.

Notices of copyright infringement, or takedown notices, may be lodged by contacting relevant ICT Officers or via the following location on the University's web site:
• http://www.imtu.edu./copyright/feedback/takedown.html

3.6. Modification of ICT Services, Facilities and Infrastructure

Network modifications shall only be made following written approval by the head of ICT or their nominees. Network modifications may only be carried out by an ICT Officer.

3.6.1. Unauthorized Modifications of ICT Services, Facilities and Infrastructure

All network modifications performed without authorization from a Senior Officer or by an unauthorized person are prohibited. Unless part of an approved network modification under section 3.7 above, the installation of a port splitter or any network communication device that supports multiple simultaneous connections to a single network port or third party network(s) is expressly prohibited.
Examples of modifications include, but are not limited to:

- Disconnecting computers from the University network;
- Connecting unregistered devices;
- Connecting hubs, switches or port splitters.

Where an unauthorized modification is detected, a breach of policy may be pursued and connectivity to a network port may be terminated.

3.7Use of Privately Owned ICT Devices

The IMTU allows Authorized Users to connect privately owned Devices to the IMTU ICT Infrastructure via connection Gateways, and allows limited connection to the IMTU staff network.

3.8Connection to Gateways

Gateways are ICT Services where Device connection has been authorized by the Chief Information Officer. Gateways are provided for the purpose of connecting privately owned Devices, and include:

i. Connect wireless; and
ii. Wired connectivity in some study areas (e.g. Learning Hubs).

Any Device that connects to IMTU Gateway must meet the following requirements:

i. Privately owned Devices may only be used on the IMTU Gateways in a legal manner and in accordance with Federal and State legislation.
ii. Users must adhere to IMTU Ordinances, Policies and Procedures whist connected to any IMTU Gateway.
iii. All Devices that support anti-virus software must have an up-to-date anti-virus package installed and operating while connected to the University network.

The IMTU shall not be held responsible for the management and maintenance of privately owned Devices connected to Gateways.

3.8.1 Connection to the IMTU Staff Network

IMTU Gateways are distinct and separate networks from the University staff network.
In cases where a privately owned Device is to be registered on the University staff network the following conditions apply:

i. The connection request must be supported by a valid reason, and made to a Senior Officer.
ii. Connections must be authorized by the Senior Officer.
iii. Access will be provided on a minimal requirements basis.
iv. Devices must have an up-to-date anti-virus package installed and operating.
v. Devices must be used in a legal manner and in accordance with Federal and State legislation.

vi. Users must adhere to IMTU Ordinances, Policies and Procedures whist connected to the IMTU staff network.

An ICT Officer must be able to provide connection support to the Device while it is connected to IMTU staff network:

i. The owner of the device must provide an account to the ICT Officer.
ii. In cases where the support of a privately owned device extends beyond connection, the device owner may be charged remuneration for that support. The charge for support is at the discretion of the Faculty, School or Division providing the connection.

3.8.2 Connection Restrictions

No privately owned device will have access to student databases, staff databases or financial systems, except where those systems provide a self- service interface for the User. Privately owned devices may only have access to ICT Services or data stores where the Data Custodian authorizes such a connection to occur, or the ICT Service or data store provides a self-service interface for the User.

3.9 Unauthorized Use

The Computer's system and networks, and provision of email and Internet facilities, must not be used for the creation, transmission, downloading, browsing, viewing, reproduction or accessing of any image, material or other data of any kind which:

a) is illegal, obscene, pornographic, indecent, vulgar or threatening;

b) contains unacceptable content, including but not limited to, sexually explicit messages, images, cartoons, jokes, or unwelcome propositions, or any other content which is designed to cause or likely to cause harassment or provocation of any other person or organization based on sex, sexual orientation, age, race, national origin, disability, religious or political belief;

c) is defamatory, slanderous or libelous;

d) deliberately introduces viruses into the email or Internet systems of the KCMUCo or any other party or is designed to deliberately corrupt or destroy the data of other users;

e) conflicts with the IMTU College's commercial interests;

f) violates the privacy of other users;

g) Infringes or may infringe the intellectual property or other rights of IMTU or those of a third party;

3.10 Connection Disclaimers

IMTU shall not be held responsible for damage or loss to privately owned Devices.

i. The IT Officer has the right to negotiate with any Senior Officer regarding the authorization of a connection request for a privately owned Device to the University staff network. Through negotiation the Chief Information Officer, has the right to reject or revoke any connection request.

ii. ICT Officers have the right to disconnect privately owned Devices from University Gateways and network in the event of a breach of this Policy or any other Ordinance, Policy or Procedure of the IMTU.

iii. The ICT Security Manager has the right to request disconnection of any privately owned Device connected to any Gateway or network of the IMTU.

3.11 Software Installation on IMTUICT Facilities and Devices

IMTU ICT Facilities and Devices operate with a standard, or known, operating environment. This environment is created and configured to allow a Device to support Authorized users in their work, and to integrate with IMTU ICT Services. Any changes to this environment, such as additional software or configuration changes, must be authorized, and preferably auctioned, by an IT Officer.

3.11.1Authorised Software

Authorized software is considered to be software that meets the following conditions:

i. The software is used in accordance with license terms;
ii. The software has been tested by an authorized ICT Officer to ensure functionality and security of ICT Facilities; the software has been installed by an authorized ICT Officer; or
iii. The installation of the software has been authorized by an ICT Officer.

3.11.2. Unauthorized Software

Unauthorized software is considered to be any software that:
i. is used in breach of software license agreements;
ii. has not been tested by an authorized ICT Officer;
iii. is not installed by an ICT Officer; or
iv. Has not been authorized by an ICT Officer.

3.11.3. Unlicensed Software

Unlicensed software is considered to be all software used outside of the license agreement that accompanies the software. The use of unlicensed software on IMTU ICT Facilities is strictly prohibited, and any instance immediately renders the software unauthorized.
The installation and use of unlicensed software cannot be authorized by any person. The software may not be installed or used until the conditions of the license have been met.

Any software installed or used in violation of license terms shall be deemed unauthorized software and will be in breach of this policy.

3.12 Privacy and Monitoring

All usage of ICT Services, Facilities and Infrastructure will be monitored. Information related to the usage of ICT Services, Facilities and Infrastructure will be stored and may be used to ensure or investigate compliance with University Policies, Procedures and Guidelines and relevant State and Federal legislation, the IMTU may collect information related to the use of ICT Services, Facilities and Infrastructure.

Further information related to the monitoring of ICT Services, Facilities and Infrastructure, and the usage of information collected, is provided in the ICT Security Policy.

3.12.1 Breaches

Breach of this Policy may result in disciplinary action, as provided for under the applicable Employment Agreements and Ordinances.

Staff, students and associates learning of any violation of this Policy are obligated to bring this matter to the attention of an appropriate staff member within the University without delay.

3.13 Responsibilities

Chief Information Officer is responsible for:

i. Implementation
ii. Compliance

Chief Information Officer and ICT Security Manager are responsible for:

i. Monitoring and evaluation
ii. Development and/or review

ICT Security Manager, together with the Legal Office is responsible for:

i. Interpretation and advice.

3.14 Review and revision of the IMTU ICT Policy

An assessment of the outcomes of this policy will provide information on the extent to which the policy is being implemented and the progress being made in achieving Policy objectives. An overall policy review will be undertaken as soon as when the need arises.

International Medical And Technological University
P.O. Box 77594
New Bagamoyo Road
Mbezi Beach Area
Dar Es Salaam, Tanzania
www.imtu.edu