



UNITED REPUBLIC OF TANZANIA
MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY
UNIVERSITY OF DAR ES SALAAM
DAR ES SALAAM UNIVERSITY COLLEGE
OF EDUCATION



INFORMATION AND COMMUNICATION
TECHNOLOGY POLICY

FEBRUARY, 2025

THE UNITED REPUBLIC OF TANZANIADar es Salaam University College of
Education (DUCE)**Document Name:** ICT Policy**Document Number:** DUCE/ICT/003

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Governing Board of the Dar es Salaam University College of Education	DUCE Governing Board		14/02/2025

PREFACE

Information and Communication Technology (ICT) plays an increasingly important role in facilitating the realization of institution's mission and vision. Consequently, in May 2019, the Dar es Salaam University College of Education (DUCE) formulated the Second Five Years ICT Policy (Second ICTP). However, after five years successful implementation of the Policy, its implementation duration has come to an end, hence a need for review. Also, while implementing the Second ICTP, the College faced some issues and challenges that affected smooth implementation of the Policy. These included, but not limited to, aging ICT facilities due to short life span of electronic and infrastructure ICT facilities; pace of technology change and its dynamicity, which require regular review of ICT policies, new implementation strategies and upgrading of ICT infrastructures, systems and applications; and a need to move towards automating core business processes so as to adhere to the e-Government Act 2019 and its Regulations of 2020. These issues and challenges necessitate to have a new ICTP, a Third ICTP.

Moreover, the College formulated the Second ICTP that would guide the College for five years, from 2019/2020 to 2023/2024. However, following the review of the College Five-Year Rolling Strategic Plan (FYRSP) 2020/2021 – 2024/2025 that resulted into approval of the College FYRSP 2021/2022 – 2025/2026, necessitated review of the Second ICTP so as to have a Third ICTP that would reflect the objectives of the newly approved FYRSP. Further to that commencement of application of the e-Government Act 2019 and its Regulations of 2020, made it necessary to review the Second ICTP and formulate the Third ICTP, to ensure comprehensive alignment to the Act and Regulations. Therefore, this Third ICTP is very well aligned to the current ICT developments and trends in the Country as well as the current legal framework. Also, the Policy is built in line with the National Policy context, including among others the National Development Vision, National Information and Communications Technologies Policy and e-Government standards and guidelines.

Therefore, it is my expectation that the College community will observe the Policy provisions for enhanced application and management of ICT infrastructure and facilities and ensure appropriate and optimal utilization of ICT applications in the College's core functions. The Policy shall guide establishment of sustainable, efficient, user-friendly, secure operations and the deployment of anticipated ICT services and resources.

Prof. Stephen Oswald Maluka

Principal

Dar es Salaam University College of Education (DUCE)

January, 2025

ACKNOWLEDGMENTS

Development and completion of this document is a result of joint efforts. I would like to express the College appreciations to all those who played role in the review of the Second ICTP and subsequent development of the Third ICTP.

Firstly, I would like to express the College appreciation to the ICT technical team for leading the process of review of the Second ICTP and formulation of this Policy document. Specifically, I thank the appointed Team for a successful accomplishment of this assignment. I understand their demanding assignment of reviewing the Second ICTP, conducting ICT environmental scanning, consulting the e-Government Act 2019 and its Regulations of 2020 and other related documents. It is because of their commitment such accomplishment was possible.

Secondly, I would like to express the College appreciation to the ICT Steering Committee. We understand the pivotal role of the Committee in ensuring successful implementation of the Second ICTP and subsequent review of the same. The Committee has provided an important oversight role of the entire process and technical advice.

I would also like to acknowledge contribution of Dr. Christina Raphael Isingo, the College Deputy Principal (Academic, Research and Consultancy) for her tireless efforts to ensure proper alignment of the Policy to the College academic, research and consultancy operations. The contributions make the Policy more useful in successful achievement of the College goals and objectives. In the same spirit, I would like to thank the College Principal, Prof. Stephen Oswald Maluka, for his oversight role to ensure that the Policy review is accomplished and a new ICTP is in place. He approved resources to be directed to this assignment and provided a general vision and outlook of the Policy document.

Lastly, I would like to thank each and everyone who participated in one way or the other in having the Third ICTP. These include the College Community and stakeholders.

It is our hope that staff, students and the entire College community will ensure successful implementation of this ICT Policy and therefore enhance the College application of ICT in its core functions for enhanced quality of services in teaching and Learning, Research, Consultancy, and Public Service delivery. Also, it will provide a comprehensive guide to the Management of ICT resources at the College.

Prof. Method Samwel Semiono

Deputy Principal – Planning, Finance and Administration

Dar es Salaam University College of Education (DUCE)

January, 2025

TABLE OF CONTENTS

PREFACE	iii
ACKNOWLEDGMENTS	iv
CHAPTER ONE	1
1. INTRODUCTION AND BACKGROUND	1
1.1. Rationale of the Review of the Second ICTP	1
1.2. Purpose and Objectives	2
1.3. Scope.....	3
CHAPTER TWO.....	4
2. SITUATIONAL ANALYSIS	4
2.1. College ICT Growth and Landscaping.....	4
2.2. Issues and challenges that need to be addressed.....	5
CHAPTER THREE.....	7
3. POLICY ISSUES, OBJECTIVES AND STATEMENTS.....	7
3.1. ICT Governance.....	7
3.1.1. Policy Issues	7
3.1.2. Policy Objectives.....	7
3.1.3. Policy Statements	7
3.2. ICT Service Management.....	8
3.2.1. Policy Issues	8
3.2.2. Policy Objectives.....	8
3.2.3. Policy Statements	8
3.3. Management of ICT Infrastructure	9
3.3.1. Policy Issues	9
3.3.2. Policy Objective	9
3.3.3. Policy Statements	9
3.3.3.1. Infrastructure Planning and Design.....	9
3.3.3.2. Data Management, Storage and Disposal	9
3.3.3.3. ICT Equipment and Hosting	9
3.3.3.4. Infrastructure Maintenance and Support	9
3.4. ICT Security and Business Continuity	10
3.4.1. Policy Issues	10
3.4.2. Policy Objectives.....	10
3.4.3. Policy Statements	11

3.5. e-learning Facilities to Support Teaching, Learning, Research and Public Service Delivery	11
3.5.1. Policy Issues	11
3.5.2. Policy Objectives	11
3.5.3. Policy Statements	11
3.6. ICT Applications Acquisition and Maintenance	12
3.6.1. Policy Issue	12
3.6.2. Policy Objectives	12
3.6.3. Policy Statements	12
3.7. ICT Capacity Building	13
3.7.1. Policy Issues	13
3.7.2. Policy Objective	13
3.7.3. Policy Statements	13
CHAPTER FOUR	14
4. IMPLEMENTATION, MONITORING, EVALUATION AND REVIEW	14
4.1. Implementation	14
4.2. Roles and Responsibilities	14
4.2.1. College Governing Board	14
4.2.2. The Accounting Officer	15
4.2.3. ICT Steering Committee	15
4.2.4. Deans'/Directors/ Managers/Head of Departments/Units	15
4.2.5. Head of ICT Unit	16
4.2.6. Head of Internal Audit Unit	16
4.2.7. Users of ICT Systems	16
4.3. Monitoring and Evaluation	17
4.4. Review	17
5. GLOSSARY AND ACRONYMS	18
5.1. Glossary	18
5.2. Acronyms and Abbreviations	22
6. BIBLIOGRAPHY	23
7. DOCUMENT CONTROL	23

CHAPTER ONE

1. INTRODUCTION AND BACKGROUND

Dar es Salaam University College of Education (DUCE) is a Constituent College of the University of Dar es Salaam (UDSM). DUCE was established as a Constituent College of UDSM through Government Notice No. 166 published on 23rd April 2010 in accordance with the Universities Act, 2005 and the University of Dar es Salaam Charter, 2007. The Order came into operation on 1st of September 2005 when the College was officially established.

The trend towards a knowledge-based economy has emphasized the importance of ICT in development efforts in educational sector. For the College to realize the value out of ICT investment, ICT must be deployed to improve efficiency and effectiveness in internal and external services delivery. This means that, a comprehensive framework established by ICTP to provide appropriate directives to harness ICT, is necessary for achievement of College's objectives. The ICTP will ensure that the ICT infrastructure and capacity are utilized effectively and are in alignment with the College's strategic objectives, National ICTP, National e-Government Strategy, the e-Government Standards and Guidelines, and the College's Rolling strategic plan 2020/2021-2025/2026.

1.1. Rationale of the Review of the Second ICTP

The College need to meet its objective of improving its services and increasing productivity by leveraging on new technologies. The College has been investing on ICT to facilitate its internal business operations including teaching and learning, research, consultancy and public services delivery so as to attain its strategic goals. The College operations are increasingly depending on ICT, making the Institution vulnerable to ICT related risks. In this regard, it is evident that, the College needs to develop and operationalize comprehensive ICT Policy to direct ICT adoption and usage within the College and compliance with e-Government Act 2019 with its Regulations of 2020 and other formulated e-Government Standards and Guidelines. It is because of these; the College has had the Second ICTP adopted in May 2019. However, after five years successful implementation of the Policy, its implementation duration has come to an end, hence a need for review. Also, while implementing the Second ICTP, the College faced some issues and challenges that affected smooth implementation of the Policy. These included, but not limited to, aging ICT facilities due to short life span of electronic and infrastructure ICT facilities; pace of technology change and its dynamicity, which require regular review of ICT policies, new implementation strategies and upgrading of ICT infrastructures, systems and applications; and a need to move towards automating core business processes so as to adhere to the e-Government Act 2019 and its Regulations of 2020. These issues and challenges necessitate to have a new ICTP, a Third ICTP.

Moreover, the College formulated the Second ICTP that would guide the College for five years, from 2019/2020 to 2023/2024. However, following the review of the College Five-Year Rolling Strategic Plan (FYRSP) 2020/2021 – 2024/2025 that resulted into approval of the College FYRSP 2021/2022 – 2025/2026 and the conducted ICT Security Maturity Assessment necessitated review of the Second ICTP so as to have a Third ICTP that would reflect the objectives of the newly approved FYRSP. Further to that commencement of application of the e-Government Act 2019 and its Regulations of 2020, made it necessary to review the Second ICTP and formulate the Third ICTP, to ensure comprehensive alignment to the Act and Regulations. Therefore, this Third ICTP is very well aligned to the current ICT developments and trends in the Country as well as the current legal framework. Also, the Policy is built in line with the National Policy context, including among others the National Development Vision, National Information and Communications Technologies Policy and e-Government standards and guidelines.

Apart from that, review of the ICTP has been triggered by enactment of Cyber Crime Act and its Regulations. This required re-alignment of the Policy to the Nation's legal framework. Also, the review was triggered by the developments in ICT field at the College whereby the Collage has improved ICT facilities, including CCTV Cameras, started to use new systems such as Library Management System, e-office, Government Mail System etc, and ICT infrastructure such as fiber optic, increasing internet bandwidth and offering internet to students' outdoor places.

1.2. Purpose and Objectives

This Policy provides the highest-level ICT directives for the College. The main purpose of this Policy is to ensure that College's ICT related investment, operations and maintenance processes and usage are well directed. The specific objectives of this policy are;

- (a) To ensure ICT governance becomes the integral part of the College governance.
- (b) ICT services provisions are in-line with College's business requirements based on existing e-Government standards and best practices.
- (c) All the College information resources and services are well secured using appropriate controls.
- (d) To ensure the members of the College use ICT facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.
- (e) Ensure that ICT is accessible to entire College community regardless of gender, physical disability, race and religion.

1.3. Scope

This Policy is applicable to all College staff, students and other users of ICT equipment and infrastructures owned or leased by the College as well as all equipment connected to College's ICT related infrastructure. This Policy is developed to complement other Government guidelines that have been issued. These include:

- (a) The Guidelines on management of public websites named: '*Mwongozo wa Kusimamia na Kuendesha Tovuti za Serikali, 2014*' and amendments made from time to time.
- (b) The Cybercrimes Act, 2015 and the subsequent Government Cyber Security Strategy 2022.
- (c) e-Government Guidelines 2017 and amendments made from time to time.
- (d) The e-Government Act 2019.
- (e) e-Government General Regulations 2020.
- (f) The Guidelines on Government Video Communication named: '*Mwongozo wa Mawasiliano kwa Njia ya Video Serikalini, 2020*' and amendments made from time to time.
- (g) Technical Standards and Guidelines for Government Websites, 2022 and amendments made from time to time.
- (h) Government e-mail naming standard, 2022. Or any other amendments made from time to time.
- (i) Government Domain Naming Standards, 2022 and amendments made from time to time.
- (j) The Guidelines on Effective and Safe Utilisation of ICT Equipment, Data and System named: '*Mwongozo wa Matumizi Bora, Sahihi na Salama wa Vifaa, Data na Mifumo ya TEHAMA Serikalini, 2022*' and amendments made from time to time.
- (k) All e-Government Technical Standards issued by the Institution responsible for e-Government implementation.

CHAPTER TWO

2. SITUATIONAL ANALYSIS

In the past five year, the College has made remarkable progress in procuring and deploying ICT equipment, systems and infrastructure. This progress is attributed to its previous ICT Policies and ICT Master Plan (that emphasized the use of ICT in dispensing academic, research and administrative functions and mandate to the ICT Unit through the ICT Steering Committee to oversee ICT development, implementation and of serving as an ICT resource management centre in general for the entire College. To have a working policy to sustain the ICT achievements acquired and foster more transformations in ICT, situational analysis is crucial. The following sections conducts such an analysis as follows:

2.1. College ICT Growth and Landscaping

The ICT landscape is meant to present current state of ICT at the College. The ICT Policy facilitated effective implementation, use and management of ICT resources at the College. Currently the following ICT resources are in place:

- (a) *Teaching and Learning, Research, Consultancy and Public Service delivery ICT facilities, infrastructure and know-how:* the College has developed capacity of staff and students for accessing e-learning materials and other online materials. The required resources that would enable staff and students to accomplish their goals were acquired in-terms of desktop computers, laptop computers, internet connectivity, and e-learning platforms.
- (b) *Access to Internet connectivity:* the College has a total bandwidth of 630 Mbps, of which TERNET and COSTECH provides 600 Mbps and 30 Mbps respectively;
- (c) *Access to shared resources via campus Fiber optic backbone and Network infrastructure:* Through the Higher Education for Economic Transformation (HEET) Project, the College constructed and installed a Fiber Optic Backbone through which major College buildings have been connected to a campus fiber optic backbone.
In addition, wireless connectivity installed at the College buildings and Open Areas including the Students Open Areas "Vimbwete."
- (d) *Access to systems application:* The college has put in-place a number of application and some are used as a Software As A Service (SAAS). These includes but not limited to Library Management Information System and Digital Library and College Journal Information System. Also, the College uses Government shared applications which includes the Human Capital Management Information System (HCMIS), Government Mailing System (GMS), 'Mfumo wa Ulipaji Serikalini' (MUSE), Government of Tanzania Health Operation Management Information System (GOTHOMIS),

e-Office, Online Helpdesk, GAMIS, PEPMIS, NEST etc. Further, the College uses centralized academic applications managed by the University of Dar es Salaam which includes Academic Register Information System (ARIS3) and Research Information Management System (RIMS). In addition, the College has a Website in place; and

- (e) *Access to computing infrastructure:* the College through the HEET Project has established the following computer labs: Education Lab (25 Computers), Science lab (50 Computers), GIS Lab (40 Computers), and Library (30 Computers).
- (f) *Installation of ICT Security Systems, Video Conferencing Facility, Special Needs Software and Hardware:* The College has installed CCTV Cameras for security purposes; it has fixed a video conferencing facility and procured facilities and programmes for students with disabilities.

2.2. Issues and challenges that need to be addressed

While implementing the Second ICTP, the College faced some issues and challenges that affected smooth implementation of the Policy. These include but not limited to the following:

- (a) *Aging ICT facilities:* Lifespan for most of active ICT facilities, such as computers, servers and switches is three years and at-most is five years. As a result, the College needs to have in place sufficient funds for maintaining and replacing aged ICT facilities. However, acquisition of such funds appears to be a challenge.
- (b) *Pace of technology change and its dynamicity:* ICT is very dynamic. New technologies are invented at rapid speed. For instance, at present we have Artificial Intelligence which pose both threat and opportunity to the organisation's operations. Since the College is not in isolation, it must adjust itself to match with technological changes. Consequently, a need for regular review of ICT policies, adaptation of new implementation strategies and upgrading of ICT infrastructures, systems and applications are crucial.
- (c) *Insufficient funding to improve ICT Infrastructure, systems applications and ICT projects:* given the requirements of ICT facilities and infrastructure at the College, the College requires huge investment to enable the implementation of earmarked projects related to ICT projects. However, due to insufficient funds available, only few projects are implemented depending on funds availability.
- (d) *Higher rates of IT staff turnover, and High remunerations for retaining them:* most of organizations in the Country are moving towards automating their core business processes. Consequently, the demand for high skilled and knowledgeable IT personnel, of whom are few in the

market, has risen. This high demand for the IT personnel has raised remuneration of such personnel. Thus, retaining them with government salary pay is a challenge.

- (e) *Resistance to change staff and students to achieve greater efficiency by taking advantage of ICT:* the paradigm shifts from manual and paper-based system to automated ones, have been adopted by the College staff and students with mixed behavioral change. Some are rigid to change to adopt technology. Consequently, this affects negatively the effective use of ICT in supporting core business of the College.

CHAPTER THREE

3. POLICY ISSUES, OBJECTIVES AND STATEMENTS

3.1. ICT Governance

3.1.1. Policy Issues

The College is one of the fastest growing higher education institutions, thus requires a well-established framework for ICT investment decisions, accountability, monitoring and evaluation. This enables attainment of quality and cost-effective ICT services to enhance efficiency of academic, research, consultancy, public services and administrative functions.

3.1.2. Policy Objectives

The Policy objectives are to.

- (a) Create a conducive environment for a vibrant and sustainable ICT infrastructure and quality ICT service delivery at the College.
- (b) Spearheading the adoption and use of state-of-the-art ICT technologies in supporting teaching, research and public service delivery.
- (c) Establish proper documentations on ICT infrastructures and critical assets including technical, policies, and procedural matters.

3.1.3. Policy Statements

The College shall:

- (a) Set up an ICT governance structure to manage ICT operations and a secure ICT environment that complies with the law, e-Government standards and guidelines.
- (b) Establish ICT Steering Committee to determine prioritisation of ICT-enabled investment programmes in line with the Institution's business strategy and priorities, track status of ICT initiatives, resolve resource conflicts and monitor ICT services.
- (c) Establish a strong ICT Unit capable of supporting strategic objectives of the institution.
- (d) Ensure that ICT Strategy for implementation of this Policy is established and operationalized.
- (e) Ensure that Management Documents are formulated in accordance to the e-Government Act and its Regulations and other related e-Government standards and guidelines.
- (f) Ensure that ICT plans fit the current and on-going needs of the College and that the ICT plans support the College strategic plan.
- (g) Ensure that management of ICT projects conforms to the Government ICT projects management procedures and complies with all internal developed procedures for managing projects.
- (h) Ensure that employees and third parties have a personal obligation to comply with internal ICT Policy, guidelines and procedures and must keep abreast of, and comply with, any changes.

- Failure to comply may result in legal or disciplinary actions.
- (i) Enhance partnership in the development and application of ICT with academic institutions, industries, government institutions and the private sector to foster innovation and address common challenges.
 - (j) Implement the necessary controls to ensure that all ICT procurements are done in line with requirements of Public Procurement Act (PPA).
 - (k) Ensure equal and equitable access to ICT assistive technology for people with Special Needs.

3.2. ICT Service Management

3.2.1. Policy Issues

ICT Service management deals with how ICT resources and core business practices altogether are delivered in such a way that the end user experiences the most desired results from accessing the entire solution stack.

3.2.2. Policy Objectives

The objectives of ICT Service Management are:

- (a) To improve internal and external stakeholders' satisfaction.
- (b) To assist in defining meaningful metrics to measure service results and using the metrics to drive continuous service improvement.
- (c) To enable the monitoring and improvement of service quality through the effective application of processes.
- (d) To ensure compliance with all e-Government Standards and Guidelines relating to the ICT Service Management.

3.2.3. Policy Statements

The College shall:

- (a) Enhance the use of an ICT Helpdesk system to ensure that business disruptions are minimised, users' queries are responded to and ICT problems are resolved. An ICT Service Management document shall be developed accordingly.
- (b) Ensure that for procured ICT services, Service Level Agreements between the providers and the College are established.
- (c) Establish mechanism to collect, analyze and report end user's feedback on ICT services.
- (d) Ensure that a robust business continuity and service recovery plans are in place and that these plans are semi-annually tested and key staff are appropriately trained.
- (e) Establish a capacity plan to monitor ICT resources usage for existing and planned systems in order to assist in time and cost-effective purchase of additional resources so as to avoid panic purchase when resources run out.

3.3. Management of ICT Infrastructure

3.3.1. Policy Issues

ICT infrastructure is the backbone for supporting the College's business operations by enabling information exchange and providing secure access to different applications. This consists of all hardware devices such as network devices, servers, workstations, laptop, storage devices, back-up, operating facilities and supporting platform like operating systems and databases.

3.3.2. Policy Objective

The objective of managing ICT Infrastructure is to ensure that the College's ICT infrastructure operations are optimized in order to deliver higher level service quality and support business-relevant operations based on ICT planning and management best practices.

3.3.3. Policy Statements

The College Shall:

3.3.3.1. Infrastructure Planning and Design

- (a) Ensure that ICT infrastructure architecture is in place and in line with the Institution's current and future requirements.
- (b) Ensure that appropriate ICT infrastructure is setup and well managed.

3.3.3.2. Data Management, Storage and Disposal

- (a) Ensure that a formal documented backup procedure is in place.
- (b) Ensure that all business-related data shall be stored in a way to facilitate back up procedures and access.
- (c) Ensure proper and safe disposal for the ICT assets as per the Government disposal procedures.
- (d) Establish mechanism for proper disposal of ICT assets and facilities through recycling or alternative use of disposed equipment.

3.3.3.3. ICT Equipment and Hosting

- (a) Acquire desktop computers, laptop, servers, printers and networking equipment from authorized suppliers.
- (b) All ICT resources shall be acquired in consultation with ICT Unit.
- (c) Ensure that approved Government environment for hosting computing and storage equipment based on standards and best practices is used.

3.3.3.4. Infrastructure Maintenance and Support

- (a) Prepare ICT Maintenance Plan and semi-annually conduct ICT maintenance.
- (b) Ensure that all ICT infrastructure components are maintained at a reasonable operational and secure level.
- (c) Ensure that standard software list including the operating system to be installed into the Institution's equipment is established.
- (d) Procure maintenance services from organization that have technical capabilities.

- (e) Ensure that network and server equipment are secured from unauthorized access from both internal and external people.
- (f) Establish mechanism to ensure that all installed ICT infrastructure including College wide network and Internet, and departmental Computer laboratories and PARs are maintained and utilized effectively.
- (g) Encourage cooperation with other institutions on responding to the challenges of convergence and newly emerging technologies, while drawing inputs together through sharing resources.
- (h) Institute measures of security that will ensure that ICT infrastructure and facilities are utilized by bona fide College community.
- (i) Ensure setting aside of funds for procurement, development, replacement, upgrading and maintenance of ICT facilities.
- (j) Encourage sharing of relevant ICT resources in order to ensure optimal utilization of ICTs in the core activities of the College.
- (k) Promote uniformity of ICT facilities at the College.
- (l) Ensure that ICT assets including ICT infrastructure, systems, applications, projects at the College are registered at the Government ICT Service Portal for proper inventory, management and easy retrieval of ICT assets and facilities.

3.4. ICT Security and Business Continuity

3.4.1. Policy Issues

ICT Security covers all the processes by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction throughout an organization.

Business continuity involves planning and preparation processes that the College undertake to ensure that it can continue operating and delivering services during and after disruptive events. Disruptive events include natural disasters, technological failures, cyberattacks, or any other unforeseen circumstances that might interrupt regular business operations.

3.4.2. Policy Objectives

The general objective of managing ICT security and business continuity is to provide the College with information security mechanism to support the achievement of its strategic goals based on best practices.

The specific objectives are:

- (a) Protection of the College's ICT resources from accidental or malicious act.
- (b) Making the College's stakeholders aware of their responsibilities with respect of ICT security.
- (c) Maintaining its ICT environment so that it remains in a running state and does not affect the business performance or services.

3.4.3. Policy Statements

The College shall:

- (a) Adhere ICT Security Policy.
- (b) Put in place measures to ensure confidentiality, integrity and availability of its ICT resources.
- (c) Adhere to guidelines and procedures for acceptable use of ICT resources at the College
- (d) Support and promote information security awareness initiatives to its students, staff and to the general public.
- (e) Grant access to the relevant College ICT resources only to bona fide College students and staff. Any other user shall seek authorization prior to accessing the resources.
- (f) Operationalize Disaster Recovery Plan for continuity of business including the implementation of redundant systems and infrastructure.
- (g) Enforce security control mechanism for physical and logical access to all critical systems and locations;
- (h) Monitor use of College ICT facilities and premises. This is to ensure that the institution's business interests are protected, for quality control purposes, to detect abuse of the systems, or to detect or prevent crime or misconduct.

3.5. e-learning Facilities to Support Teaching, Learning, Research and Public Service Delivery

3.5.1. Policy Issues

e-learning is the use of ICT to enhance and/or support learning in education. e-learning is important technology to improve the quality of teaching and enhance the academic profile. Utilization of e-learning resources and technologies enhances motivation and provides new instructional stimulus for the learners. e-learning is important technology to improve the quality of teaching and enhance the academic profile.

3.5.2. Policy Objectives

e-learning has several key objectives aimed at creating an effective, efficient, and inclusive educational environment that leverages technology to overcome traditional barriers to learning.

3.5.3. Policy Statements

The College shall:

- (a) Ensure strategies and related guidelines for improving e-learning teaching and learning supporting environment are in place to serve better more students and staff in a sustainable manner.
- (b) Promote creation and development of new ICT applications and multimedia content to support teaching, learning and research by encouraging and rewarding ICT related research and development

initiatives.

- (c) Encourage enhancement of strategies for ICT awareness campaign to support effective use of ICT to students and staff; and that they are trained on a continuing basis to equip them with the requisite skills to fully exploit the Digital Learning Environment (DLE).
- (d) Promote digital inclusion technologies for people with special needs.

3.6. ICT Applications Acquisition and Maintenance

3.6.1. Policy Issue

ICT Applications are software designed for end-users to use in their daily operations to support the College business processes.

3.6.2. Policy Objectives

The general objective of managing ICT applications is to ensure that ICT applications that are in use or to be acquired address the functions requirements of the College and effective working as intended to provide reasonable return on College investment. Specific objectives are:

- (a) To ensure system acquisition follow proper procedures;
- (b) To establish controls for efficient acquisition and administration of applications;
- (c) To enhance accountability on the management and usage of ICT applications.
- (d) Ensure that the duplication of efforts is minimized for efficient and cost-effective development, management, control, maintenance and usage of ICT applications at the College.

3.6.3. Policy Statements

- (a) Develop ICT Acquisition, Development and Maintenance Guidelines
- (b) User departments shall submit to ICT Unit their ICT requirements to be included in ICT application.
- (c) All applications supplied shall be checked by ICT Unit to verify if the technical requirements established are met and approved.
- (d) ICT Unit shall establish appropriate software standards to facilitate acquisition/development.
- (e) Administration and maintenance of applications shall be an on-going process that will last throughout the life cycle of the application.
- (f) Every application acquired by the College shall have documentation in place and updated regularly.
- (g) Develop Change Management Procedures to include installation of additional applications or overriding existing one
- (h) Software acquired for installation into the College equipment shall be licensed and also comply with Government guidelines. The acquisition of Open-Source Software (OSS) related products and services shall be made in consultation with the ICT Unit.

- (i) Ensure that any issuance of utilization rights such as software utilization permission right, reproduction right, copyright, patent etc. are properly documented and duly approved by the relevant authority;
- (j) Ensure that all software and documentation developed by College staff in the course of employment are exclusive property of the College. And that the College can sell, exchange or donate software to other agencies in accordance with applicable College guidelines, e-Government standard and guidelines and Government regulations for Asset Management.

3.7. ICT Capacity Building

3.7.1. Policy Issues

Capacity building in human resources (HR) for information and communication technology (ICT) involves developing and enhancing the skills, knowledge and capabilities of technical staff and end users to effectively use and manage ICT resources. For example, inability of users to follow simple instruction to regularly update protection software against worms and viruses.

3.7.2. Policy Objective

Training in Information and Communication Technology (ICT) aims to achieve several key objectives:

- (a) Equip staff and students with the fundamental and advanced skills needed to use computers, the internet, and digital tools programming, cybersecurity, data analysis, and network management effectively in order to increase efficiency and productivity
- (b) Foster an attitude of continuous learning and adaptation in the face of new ICT developments, online safety, privacy, and ethical issues.

3.7.3. Policy Statements

The College shall:

- (a) Recruit qualified candidates, train and re-train in-service technical staff in new emerging ICT areas regardless of gender, physical disability, race, and religion.
- (b) Strive to retain trained and competent ICT staff versed with current state of the art technology in ICT and the College requirements.
- (c) Encourage the participation of end-users in contribution to the specifications and design of the ICT applications at the College.
- (d) Provide funding and resources to support staff with innovative ICT projects.
- (e) Engage in exchange programs or collaborative projects to enhance skill development.
- (f) Encourage staff and students to learn from open-source technologies.
- (g) Encourage participation in ICT capacity-building initiatives organized by ICT Stakeholders e.g. COSTECH, eGA.

CHAPTER FOUR

4. IMPLEMENTATION, MONITORING, EVALUATION AND REVIEW

4.1. Implementation

This document shall come into operation once tabled and agreed in the College Governing Board and approved in its first page, and then shall be considered mandatory for all College's business operations.

- 4.1.1. The policies described provide top level issues for common understanding of adoption and usage at the College based on e-Government standards and guidelines and where necessary detail procedures could be developed.
- 4.1.2. An ICT Strategy shall be formulated for implementation of this Policy. From the ICT Strategy, an annual action plan shall be established and quarterly implementation report presented at the ICT Steering Committee meetings.
- 4.1.3. The College Management will use this Policy and its implementation Strategy in conjunction with the ICT Enterprise Architecture, ICT Security Policy, ICT Security Guidelines, ICT Service Management Guidelines, Business Continuity and Disaster Recovery Plan, ICT Project Management Guidelines and ICT Acquisition, Development and Maintenance Guidelines and all other related policies and guidelines to ensure that it operated within a well geared ICT ecosystem.
- 4.1.4. All employees and other authorized users of the College shall comply with requirements of this Policy.
- 4.1.5. The College community (staff, student or vendor) found to have violated this Policy may be subject to withdrawal and/or suspension of systems and network privileges or disciplinary action in accordance with rules defined by College or Government Regulations.

4.2. Roles and Responsibilities

4.2.1.College Governing Board

- 4.2.1.1. Approve ICT Policies such as ICT Strategy, Enterprise Architecture and ICT Security Policy.
- 4.2.1.2. To direct and allocate resources for ICTP implementation at the College.
- 4.2.1.3. To act as sole owner of the College ICT infrastructure and facilities; and
- 4.2.1.4. To ensure Management's compliance to the Government ICT related Acts, Regulations, Guidelines and Procedures.

4.2.2.The Accounting Officer

- 4.2.2.1. Appoint an ICT Steering Committee and determine its terms of reference.
- 4.2.2.2. To oversee implementation of the ICTP.
- 4.2.2.3. To mobilize funds for acquisition, upgrading and maintenance of ICT facilities and infrastructure.
- 4.2.2.4. To develop plans for ICTP implementation; and
- 4.2.2.5. Ensure implementation of the ICT Policy and all other ICT related Policies, Strategies and guidelines.

4.2.3.ICT Steering Committee

The Committee shall:

- (i) To review and approve ICT Policies and Strategy of the College, followed by relevant approval requirements.
- (ii) To ensure alignment of ICT with College's business needs so that ICT initiatives and services facilitate achievement of College's strategic objectives.
- (iii) To review and provide advice on ICT investment portfolio and priorities with a view of attaining value delivery.
- (iv) To ensure all ICT related risks are properly managed, this includes reviewing and approving College Business Continuity and Disaster Recovery Plan and ensure its effective implementation.
- (v) To ensure e-Government guidelines and standards are implemented by the College in order to meet compliance requirements.
- (vi) To ensure optimal resources utilization in ICT Initiatives implementation, including proper management of infrastructure, human capital and finance.
- (vii) To undertake continuous monitoring and evaluation of institutional ICT projects to ensure the anticipated benefits are realized.
- (viii) To approve any other College sub-committee as may, from time to time, be constituted and address specific ICT related matters.
- (ix) To prepare and submit quarterly ICT progress report to the e-Government Authority; and
- (x) To perform such other functions as may be directed by the Governing Board, Accounting Officer or e-Government Authority.

4.2.4.Deans'/Directors/ Managers/Head of Departments/Units

- 4.2.4.1. Shall ensure that all users under their supervision are aware and comply with this Policy and other related ICT Policies that shall be formulated.
- 4.2.4.2. Shall provide adequate and appropriate protection of ICT assets and resources under their control.

- 4.2.4.3. Shall ensure availability, integrity and confidentiality of information produced by systems under their areas of functional responsibilities and thereby ensure continuity of operations; and
- 4.2.4.4. Shall be custodian of "Data and Information" for their respective Directorates/Faculties/Departments/Sections/Units.

4.2.5. Head of ICT Unit

Subject to general oversight of the College Governing Board, the Accounting Officer and advice of the ICT Steering Committee, the Head responsible for ICT shall oversee the overall implementation of this Policy; and in particular he/she shall:

- 4.2.5.1. Initiate and coordinate the review and amendment of this Policy, as and when required in order to accommodate new technologies or services, applications, procedures and perceived dangers.
- 4.2.5.2. Plan and develop all ICT related policies/ guidelines in accordance to the e-Government Act and its Regulations.
- 4.2.5.3. Keep abreast of ICT developments in respect of ICT industry in general and College's systems in particular.
- 4.2.5.4. Recommend procedures, standards and policies for effective implementation of this Policy in line with e-Government Standards and Guidelines; and
- 4.2.5.5. Be the custodian of all ICT resources of the College including those centrally stored in server room/data centre.

4.2.6. Head of Internal Audit Unit

- 4.2.6.1. Shall audit the ICT function of the College and ensure compliancy with the Policy. To provide assurance to the Accounting Officer on matters related to ICT; and
- 4.2.6.2. To provide consultation services to the College Management on matters related to ICT compliance.

4.2.7. Users of ICT Systems

- 4.2.7.1. Shall be responsible to safeguard ICT assets of the College in their custody; and
- 4.2.7.2. Shall comply with this Policy.

4.3. Monitoring and Evaluation

ICT Steering Committee shall meet quarterly to monitor and evaluate the achievements in ICT initiatives against College ICT Policy through an ICT Strategy annual action plan and other ICT related policies that shall be formulated in accordance of their formulated Annual Action Plans.

4.4. Review

This Policy shall be reviewed within five years, or whenever there is change in the business/processes to reflect both the internal and external environment. A mid-review of the five years shall be performed to determine reviews that in a way that affects the current Policy.

5. GLOSSARY AND ACRONYMS

5.1. Glossary

Accountability	When a specific action is associated with an individual.
Application	A software program or group of software programs designed to work together to accomplish specific business objectives.
Approved software	Software that has been reviewed and deemed acceptable by the Authority for use with its ICT resources
Authorization	The process of determining whether or not an identified individual or class has been granted access rights to an information resource, and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.
Authentication	The process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.
Availability	The principle that authorized users have access to information and assets.
Assistive Technology	Is an umbrella term for assistive products and their related systems and services. Assistive technology is of fundamental importance for persons with permanent or temporary functional difficulties as it improves their functional ability, and enables and enhances their participation and inclusion in all domains of life.
Business Continuity	Is a set of planning, preparatory and related activities which are intended to ensure critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.

Confidential Information and/or Confidential Data	Information/Data that are exempted from disclosure under the provisions of applicable state and federal law.
Confidentiality	The principle that information is accessible only to authorized personnel.
Critical Information Resources	The resources determined by UCC management to be essential to its critical mission and functions, the loss of which would have an unacceptable impact.
Data confidentiality	Ensuring that information is only available to those who are authorized to have access to it.
Data integrity	Safeguarding the accuracy and completeness of information and Software.
Documentation	Means of conveying information to users in a clear and understandable manner.
Digital Assistive Products	Products occurring in the form of software and apps that support interpersonal communication, access to information, daily time management, rehabilitation, education and training.
e-Learning	A process of learning via computers over the Internet and intranets. Also referred to as Web-based training, online learning, distributed learning, or technology for learning.
e-Commerce	Business communication and transactions conducted over networks and through computers. As most restrictively defined, electronic commerce is the buying and selling of goods and services, and the transfer of funds, through digital communications.
End-User	A person who uses ICT services or the information they produce to support his/her 'normal' daily work.
Fiber-Optic Cable	Cable incorporating a number of very thin strands of glass on which information is conveyed in the form of

pulses of light.

ICT Policy	A document that elaborates on the Public Institution's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the entire ICT Management Framework, commonly known as ICT Policy of an Institution.
ICT Security	Protection of information assets through the use of technology, processes, and training, and some have also thought of security as the degree of resistance to, or protection from, harm and it applies to any vulnerable and valuable asset of any organization DUCE being one of them.
ICT Infrastructure	Network devices, server hardware, and host operating systems.
Integrity	The principle that ensures that information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information
Information and Communication Technologies (ICT)	Fusion of computers and telecommunications. Computers enable people to Work creatively, but they are limited by what they can access. Adding a communications channel, such as the Internet or other information services, significantly extends the capability of the computer. It allows it to be not only an inexpensive communications device, but also a means of obtaining education, information, and working creatively with others irrespective of geographical barriers.
Information Security	Refers to the preservation of Confidentiality – protecting information from unauthorized access and disclosure; Integrity – safeguarding the accuracy and completeness of information and processing methods; and Availability – ensuring that information and associated services are available to authorized users when required.
Multimedia	Systems that support the interactive use of text, audio, still images, video, and graphics. Each of these

elements must be converted in some way from analog form to digital form before they can be used in a computer application. Thus, the distinctive feature of multimedia is the convergence of previously diverse systems.

Online Learning	Any learning experience or environment that relies upon the Internet/WWW (World Wide Web) as the primary delivery mode of communication and presentation.
Open-Source Software (OSS/FS)	OSS/FS programs are programs whose licenses give users the freedom to run the program for any purpose, to study and modify the program, and to redistribute copies of either the original or modified program (without having to pay royalties to previous developers).
Policy	A high-level statement of organizational beliefs, goals, and objectives and the general means for their attainment in a specified subject area.
Public Information	Refers to any information approved by the management to be disclosed to members of the public.
Restricted Information	Refers to any information that is confidential information under DUCE regulations and that, due to privacy or other concerns, access to which must be limited to only authorized users and strictly monitored and controlled at all times.
Standards	A specific set of practices or procedures to regulate how a system or organization provides services.
Standard Hardware	A list of approved hardware.
Standard Software	A list of approved software.
Supervisor	Refers to any DUCE staff given supervisory responsibilities.
Steering Committee	Refers to the Committee of the Management that is responsible for overseeing the day-to-day operations of the Information and Communication Technology

Vendor/Third party	Refers to suppliers, consultants and any person or organization contracted to supply computer hardware or software, maintenance services or consultancy services
--------------------	--

5.2 Acronyms and Abbreviations

APs	Access Points
COSTECH	Tanzania Commission for Science and Technology
DLE	Digital Learning Environment
DUCE	Dar es Salaam University College Education
e-Commerce	Electronic Commerce
e-Government	Electronic Government
eGA	Electronic Government Authority
FYRSP	Five-Year Rolling Strategic Plan
GAMIS	Government Asset Management Information System
ICT	Information and Communication Technology
LAN	Local Area Network
NEST	National e-Procurement System of Tanzania
PEPMIS	Public Employee Performance Management Information System
OSS	Open-Source Software
PAR	Public Access Room
PCs	Personal Computers
TERNET	Tanzania Education and Research Network
UDSM	University of Dar es Salaam

6. BIBLIOGRAPHY

e-Government Act (2019), United Republic of Tanzania
 e-Government Regulations (2020), United Republic of Tanzania
 Creation of Government ICT Management Documents – Technical Guide
 Document Number eGA/EXT/AVS/003, e-Government Authority (eGA),
 available at <https://www.ega.go.tz/standards>
 eGA ICT Policy Sample, e-Government Authority (eGA),
<https://www.ega.go.tz/standards>
 Dar es Salaam University College of Education (DUCE) ICT Policy, 2019
 Dar es Salaam University College of Education (DUCE Five Year Rolling
 Strategic Plan 2021/2022 - 2025/2026

7. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 3.0	ICT Policy	Review and Develop ICT Policy	February, 2025
Ver. 2.0	ICT Policy	Review of ICT Policy	June, 2019
Ver. 1.0	ICT Policy	ICT Policy Document Creation	September, 2014