



UNIVERSITY OF DAR ES SALAAM
DAR ES SALAAM UNIVERSITY COLLEGE OF EDUCATION (DUCE)

ACCEPTABLE ICT USE (ICT SECURITY) GUIDELINES

MAY, 2026

THE UNITED REPUBLIC OF TANZANIA

Dar es Salaam University College of Education (DUCE)

Document Name: Acceptable ICT Use (ICT Security) Guidelines**Document Number:** DUCE/ICT/007

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	PROF. WILLIAM A.L. ANANGISYE	CHAIRPERSON DUCE BOARD		14/5/2026

TABLE OF CONTENTS

GROSSARY AND ACRONYMS	v
Glossary	v
Acronyms	v
CHAPTER ONE	1
OVERVIEW	1
1.1 Introduction	1
1.2 Objectives	1
1.3 Scope	2
1.4 Disclaimer	2
CHAPTER TWO	3
ICT ACCEPTABLE USE (ICT SECURITY) GUIDELINES	3
2.1 Unacceptable Behaviour	3
2.2 Use of ICT Assets	4
2.3 Email Security	5
2.4 Internet and Intranet Usage	8
2.5 Use of Passwords and Authentication	10
2.6 Security of ICT Equipment	11
2.7 Mobile Device Usage	12
2.8 Anti-Virus Process	13
2.9 Closed Circuit Television (CCTV) Usage	13
2.10 Access Controls	14
2.11 Software Use and Licensing	15
2.12 Technology Equipment Disposal	16
2.13 Employee Workplace Practices and User Account Termination	16
2.14 Management of Third Parties	17
CHAPTER THREE	18
IMPLEMENTATION, REVIEW AND ENFORCEMENT	18
3. Implementation and Review	18
3.1 Roles and Responsibilities	18
3.2 Monitoring and Evaluation	18
3.3 Enforcement	18
4. BIBLIOGRAPHY	Error! Bookmark not defined.
5. DOCUMENT CONTROL	20
APPENDICES-PROCUDERES AND STANDARDS	21

Appendix I: Standard for Secure Passwords and Authentication Practices	22
Appendix II: Software Installation and Licensing Procedures on College ICT	
Resources	24
Appendix III: Network Security Guidelines Standards.....	26
Appendix IV: ICT Software Patching Procedure Form.....	28

GLOSSARY AND ACRONYMS**Glossary**

Users	–	refers to all College Stakeholders including College employees and students, and third parties (contractors, visitors, interns, filed students) who make use of any ICT resources at the College.
System Administrator (SA)	–	refers to ICT staff regardless of their job descriptions and titles.
Designated System Administrator (DSA)	–	refers to ICT staff who has been commissioned to administer various computer systems at the College
Government Classification (GC1)	–	refers to a government information security level for Publicly Accessible Document.
NGAO	–	Is the official government developed secure Two-Factor Authentication (2FA) application, designed to protect digital accounts including the Government Mailing System (GMS), e-office.

Acronyms

2FA	–	Two-Factor Authentication
AHRM	–	Administration and Human Resource Management.
BIOS	–	Basic Input/Output System
CCTV	–	Closed Circuit Television System
CSIRT/CERT	–	Computer Security Incident/Emergency Response Team
DSA	–	Designated System Administrator
DUCE	–	Dar es Salaam University College of Education
GB	–	Gigabyte
GC	–	Government Classification
GMS	–	Government Mailing Systems
ICT	–	Information and Communication Technology
IDS	–	Intrusion Detection Systems
ISP	–	Internet Service Providers
MFA	–	Multi Factor Authentication
PMR	–	Password Management Request
PC	–	Personal Computer
SA	–	System Administrator
UPS	–	Uninterrupted Power Supply
USB	–	Universal Serial Bus

CHAPTER ONE

OVERVIEW

1.1 Introduction

Information and Communication Technology (ICT) plays an increasingly important role in the realisation of the College's mission and vision. Specifically, ICT ensures Confidentiality, Integrity and Availability (CIA) of information assets to support the College's core business functions. The College recognises that ICT security is a concern of the whole College community for them to benefit from ICT investments. Since technology can enable rapid spread of attacks and exploits, which can undermine the success and performance of the College, the College decided to review the ICT Security Policy (2019).

In order to manage the risks associated with ICT, this Policy requires that the College formulate guidelines Acceptable ICT Use guidelines also known as ICT Security Guidelines which outline appropriate use of the College's ICT resources, which include computers, programs, data, Local Area Network, emails, CCTV, intranet and the internet. The guidelines specifically outline acceptable practices for users of ICT resources that include employees, students and other stakeholders.

Proper implementation of these guidelines will the College meet its expectations by providing better services more quickly and at lower cost, increasing accountability among the College users and strengthening the protection of College information and confidential data.

1.2 Objectives

The Acceptable ICT Use guidelines intend to enable users to properly use and secure the College ICT resources by familiarising with the acceptable and unacceptable behaviours, conducts and practices in the use of the resources, and sanctions for failure to comply with the acceptable behaviours.

The Guidelines are specifically intended to:

- i. ensure that ICT resources and services are used in an appropriate and responsible manner;
- ii. ensure that only authorised users have access to the ICT resources through the use of password controls, door access cards etc;
- iii. safeguard the integrity and security of ICT resources; and
- iv. ensure consistent understanding of users' responsibilities and limitations when using ICT resources and services.

1.3 Scope

These Guidelines apply to all users of the College ICT resources including employees, students, and other authorised users/stakeholder.

1.4 Disclaimer

This document provides guidance on the proper use of ICT resources at the College; however, it is not by any way exhaustive. All users are obliged to comply with this guideline, the College ICT Policy (2025), ICT Security Policy (2026) and Government ICT-related Policies and Guideline.

CHAPTER TWO

ICT ACCEPTABLE USE (ICT SECURITY) GUIDELINES

The College considers ICT security a crucial undertaking to safeguard its ICT resources by mitigating the associated risks and enabling users to perform their daily duties effectively and efficiently. As such, students, employees and other stakeholders are required to make good use of ICT resources while observing ethics and security guidelines to the fullest extent in pursuit of the College's goals and objectives.

2.1 Unacceptable Behaviour

- 2.1.1 Creation, display, production, down-loading or circulation of offensive material in any form or medium.
- 2.1.2 Failure to adhere to the terms and conditions of all license agreements relating to ICT resources used including software, equipment, service documentation and other goods.
- 2.1.3 Deliberately introducing viruses, worms, trojan horses or other harmful or nuisance programs or file into any College ICT facility, or taking deliberate action to circumvent any precautions taken or prescribed by the College.
- 2.1.4 Loading into the College ICT resources any device or software without permission from the Deputy Principal (Administration).
- 2.1.5 Installation on any personal ICT facility College's Information Systems without permission from the Deputy Principal (Administration).
- 2.1.6 Removing or interfering with output of the ICT resources belonging to another user.
- 2.1.7 Failure to note and report on any observed or suspected security incidents, security weaknesses or threats.
- 2.1.8 Allowing unauthorised person to use resources assigned to the user without prior authorisation.
- 2.1.9 It is further unacceptable for any person to use College's ICT resources:
 - i. in furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
 - ii. for any political purpose;
 - iii. for any commercial purpose;
 - iv. to send threatening or harassing messages, whether sexual or otherwise;

- v. to access or share sexually explicit, obscene, or otherwise inappropriate materials;
- vi. to infringe any intellectual property rights;
- vii. to gain, or attempt to gain, unauthorised access to any computer or network;
- viii. for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
- ix. to intercept communications intended for other persons;
- x. to misrepresent or impersonate either the College or a person's role at the College;
- xi. to distribute chain letters, spam emails;
- xii. to access online gambling sites; and
- xiii. to libel or otherwise defame any person.

2.2 Use of ICT Assets

- 2.2.1 Users shall not disclose, or disseminate to unauthorised person, any information or data that they came across during system access unless it is for public consumption.
- 2.2.2 Users shall not access or try to access information other than what was granted to access.
- 2.2.3 Users shall ensure that any discarded information or data is properly disposed.
- 2.2.4 Users shall not upload any business files to personal Internet sites or via personal email/social media as they put the data out of College control that may result in leakage of confidential information.
- 2.2.5 Users shall not use any College ICT resources for any personal activities that are prohibited under the law.
- 2.2.6 Messages, postings and blogs shall not disclose any proprietary or confidential information about College or College's clients, including client contract information, internal policies, standards, procedures, processes, guidelines or financial information.
- 2.2.7 Any comments or postings made regarding user's colleagues or other individuals shall not breach their rights, including the right to data privacy, and shall not adversely affect the College reputation.

- 2.2.8 Users shall not accept offers of software upgrades or security patches from pop-up windows that appear when browsing the Internet, as these often contain malware.
- 2.2.9 The College shall not provide backup arrangements for personal applications and downloads, but may provide any support to help manage employee personal files.
- 2.2.10 Any downloaded software, music or other data, which is for personal use, that is found to or is suspected of interfering with the performance of the College's computer/network or is inappropriately licensed shall be removed from the computer by SA.
- 2.2.11 All users of workstations, PCs and laptops should ensure that their screens are clear of data when not in use. Moreover, computers should be set so that they automatically switch to a standby mode after a period of inactivity. A password should be needed to regain access to the screen.
- 2.2.12 Users should ensure that they log off and shut down, if they expect to be away from their desk or work area for a prolonged period and at the end of the working day before they leave office premises.
- 2.2.13 All software development, acquisitions, deployment and usage at the College should be coordinated centrally by ICT Unit to ensure conformity to predefined standards.
- 2.2.14 Before acquiring any software to be used by the College, users should seek audience with the ICT Unit for proper guidance.
- 2.2.15 On acquiring software, proper procurement procedures should be followed as stated in the Public Procurement Act and its Regulations.
- 2.2.16 All software acquired by DUCE should have documentation manuals and bear legitimate licenses.
- 2.2.17 Return of ICT Assets-All employees of the College and external party users must return all College ICT assets in their possession upon termination of their employment, contract or agreement.

2.3 Email Security

- 2.3.1 College's employees should have official Government email address that will be provided by the ICT Unit.
- 2.3.2 Use Government email strictly for official Government activities only.
- 2.3.3 Do not send or distribute "chain letter" type messages through Government email addresses.

- 2.3.4 Do not forward non-government information once received.
- 2.3.5 Do not use Government email to distribute information that violates Public Service ethical standards.
- 2.3.6 Send Government information or records via email only to those authorised to receive, read, and act upon them.
- 2.3.7 Return any email received through a government address that does not concern you to the sender; if the sender confirms it was sent by mistake, the message should be deleted immediately.
- 2.3.8 Do not use Government email to register on social media platforms such as Twitter, Facebook, YouTube, WhatsApp, Instagram, etc. except for the social media accounts owned by the College.
- 2.3.9 Do not use personal email addresses for communication related to Government activities.
- 2.3.10 Emails addressed to other Institutions or to individuals outside the College must clearly identify the sender by full name, position and contact address at the College. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the computer recycle bin.
- 2.3.11 If users suspect or discover e-mail containing computer viruses or phishing attacks, they should report the incident to the SA.
- 2.3.12 Users should not open or forward any e-mail from unknown or suspicious sources.
- 2.3.13 The e-mail system should not be used to commit unlawful and illicit acts.
- 2.3.14 Users should avoid publishing e-mail address to unknown individuals or expose users' credentials by filling forms from dubious links and websites.
- 2.3.15 Users should use separate e-mail addresses different from their office e-mail addresses when participating in public newsgroup or chat rooms, to avoid their office e-mail addresses and/or mail systems to become a target of spam.
- 2.3.16 Users should not reply to spam because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic.
- 2.3.17 Users should control spam by using e-mail filtering tools in e-mail software that allow users to block or screen out spam by defining some simple filtering rules.
- 2.3.18 User should not send e-mails using another person's e-mail account.

- 2.3.19 The College reserve the right to inspect, monitor and disclose the contents of any email created, sent, received or forwarded by using the College computer network or email system.
- 2.3.20 Users must not spoof or otherwise falsify a sender address.
- 2.3.21 Users are not authorised to try and gain access to another employee's data files and email without the consent of the latter.
- 2.3.22 Users are not permitted to send electronic mail that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or criticism of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- 2.3.23 If an employee vacates the College for any reasons provided, he or she is no longer the College beneficiary, the office of the AHRM should officially communicate this information to ICT Unit and thereafter the employee's DUCE email account will be disabled accordingly.
- 2.3.24 Users should not share email account passwords. For officers using management emails must handle the email account to another officer and report to the ICT Unit for issuance of a new password by sending mail to ictsupport@duce.ac.tz.
- 2.3.25 Email Retention
- i. Official email information sent or received from the GMS server shall be retained or backed up in accordance to e-Government applicable policies;
 - ii. Spam messages should not be retained.
 - iii. Appropriate official electronic message should be saved. Users are strictly forbidden from deleting an email in an attempt to hide any violation. Further, an email must not be deleted when there is an active investigation or litigation where such an email may be required to be produced in such litigation.
 - iv. Email sent to or received from certain public or government entities may be considered a public record.
- 2.3.26 Mail Quota Management
- i. The staff mail account storage size must be limited to what is reasonable for each employee. The College shall allocate an adequate mail quota size minimum of 2 GB and shall monitor its utilization for timely addition before it is fully utilized. Storage limits may vary from one employee to another depending on the usage needs.

- ii. Email should be retained and backed up. Unless otherwise indicated, for the purposes of backup and retention, an email should be considered operational data.
- iii. Users are encouraged to delete emails periodically when such emails are no longer needed. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the College to acquire storage and backup unnecessary email messages.

2.4 Internet and Intranet Usage

- 2.4.1 Internet access shall be provided to users to support daily activities upon being issued with access credentials.
- 2.4.2 For College stakeholders other than employees and students, the hosting employer will be required to send mail to ictsupport@duce.ac.tz to request for credential access for the stakeholder.
- 2.4.3 Unless specifically authorised, on item-by-item basis, users are strictly prohibited to use the Internet for:
 - i. Downloading games or shareware programs.
 - ii. Ordering (shopping) of personal items or services.
 - iii. Playing any games or participating in any on-line contest or promotion.
 - iv. Deliberately propagating computer viruses, worms, Trojan horses or trap door.
 - v. Disabling or overloading any computer system or network or attempting to disable, defeat or circumvent any system intended to protect the privacy or security of another user.
 - vi. Downloading or distributing pirated software or data.
- 2.4.4 The use of the Intranet is intended exclusively for the work undertaken for or by the College.
- 2.4.5 Users should act responsibly and maintain the integrity of the data/information within the Intranet/Internet all the time.
- 2.4.6 All information/data posted to the Intranet/Internet should be checked for malicious software.
- 2.4.7 Internet usage activities of users may be monitored by the ICT team.
- 2.4.8 Users are expected to protect their personal user credentials, such as user IDs and passwords. These should in no case be given to anyone (including colleagues) or stored on Internet browsers.

- 2.4.9 Users shall not access College confidential data via a public computer such as in a cybercafé.
- 2.4.10 It is strictly prohibited to download unapproved software using the College Internet access and install the same on College devices.
- 2.4.11 Users shall not use College Internet access to download movies, pictures and music files unless they are work-related.
- 2.4.12 All files downloaded from the Internet should be scanned using dependable anti-virus detecting software before they are opened on College devices.
- 2.4.13 Users must not deliberately try to bypass security controls on the College systems to access the Internet.
- 2.4.14 Users are not allowed to disable the anti-virus protection running on their computers for browsing the Internet.
- 2.4.15 Users shall not use the Internet resources provided to them at work for sexual or racial harassment.
- 2.4.16 Users must not use the College Internet to gain unauthorised access to other systems or websites.
- 2.4.17 Users of portable devices accessing the Internet from public places should make sure that proper security measures are maintained, such as not connecting to unsecured networks.
- 2.4.18 Users are expressly forbidden from making unauthorised alterations or extensions to the network.
- 2.4.19 A register of network devices, their access restrictions and the protocols in use should be kept by the DSA.
- 2.4.20 All changes to network configurations should be recorded in the confidential register, along with authorisation for the changes.
- 2.4.21 Users should be permitted to use only those network addresses issued to them by the DSA.
- 2.4.22 Virtual networks should be set up for specific groups of users. These groups should have Group User Access Profiles, on which the user access profiles of individual team members should be based.
- 2.4.23 Remote College users should connect to servers using a secure communication channel such as Virtual Private Network on dedicated communications lines with end-to-end encryption.

- 2.4.24 Results/Logs from the firewall should be reviewed by DSA to confirm there have been no unexpected attempts to connect.
- 2.4.25 Users should not extend or re-transmit network services and traffic in any way i.e. they should not install a router, switch, hub, or wireless access point to the system network without approval.
- 2.4.26 Users with administrative privilege should not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, system users should not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the system network infrastructure.

2.5 Use of Passwords and Authentication

- 2.5.1 Access rights to some College ICT resources will be granted through secret authentication methods, commonly the username(s) and password(s), thus the College ICT facility users;
 - i. Must not use another user's username or password, nor allow any password issued to them to be known to any other person.
 - ii. Must not leave ICT resources unattended after logging in.
 - iii. Must notify the designated authority of any change in their status which may affect their right to use ICT resources.
 - iv. Must ensure passwords used are not based on personal information like family names, year of birth or login name.
 - v. Must ensure that passwords are alphanumeric, i.e. include numbers, upper- and lower-case letters and special characters.
- 2.5.2 All User ID and default passwords supplied by third parties must be changed following the installation of the software.
- 2.5.3 For Password Management Request (PMR), users acquiring new passwords for various accesses at the College should send email to ictsupport@duce.ac.tz
- 2.5.4 Two-Factor Authentication (2FA) such as NGAO shall be enforced on as per e-Government Authority directives.
- 2.5.5 Users should adhere to Password and Authentication Guideline as per **Appendix I**.

2.6 Security of ICT Equipment

- 2.6.1 Users shall be responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use.
- 2.6.2 Any equipment or media taken off the premises of the College shall not be left unattended in public place. While travelling, users of portable devices are responsible for ensuring that proper physical handling is maintained. It is advisable to keep visual control over these devices at all times. For example, laptops should be carried as hand luggage and disguised where possible when travelling or should not be left in car back seats as they can easily be stolen.
- 2.6.3 Missing or stolen ICT equipment should be immediately reported to the SA and Police, and then other internal reporting processes should continue.
- 2.6.4 Users must take every precaution to avoid damage to equipment caused by eating or drinking in its vicinity.
- 2.6.5 ICT equipment must be switched off properly before leaving the office.
- 2.6.6 Users are not allowed to alter any software or hardware installation.
- 2.6.7 Users of the College ICT equipment in public areas shall take proper safeguards to ensure that unauthorised viewing of confidential or secret data is avoided by ensuring that their device is not left unattended, screens are locked when not in use and confidential information is not displayed on screens in public areas.
- 2.6.8 Off-premise laptops containing confidential information shall be protected with an appropriate form of access protection, e.g. passwords, smart cards, or encryption, so as to prevent unauthorised access.
- 2.6.9 Users shall observe manufacturers' instructions for protecting equipment at all times, for example, necessary precautions should be taken to protect equipment against exposure to strong electromagnetic fields.
- 2.6.10 In the event that the user faces an operational or security incident, they should immediately report it to the SA through phones or email ictsecurity@duce.ac.tz or as per the ICT Security Incidents and Management Procedures.
- 2.6.11 Rooms that host servers should be non-smoking zones, fireproof, fitted with smoke detectors and automatic or portable fire extinguisher systems.
- 2.6.12 Smoke detectors and fire extinguishers should be regularly tested and maintained to ensure that they are in good order and all tests and maintenance have to be documented.

- 2.6.13 Inflammable materials should be disposed of and documents which are still in use should be stored in a secure place.
- 2.6.14 Activities, such as rewiring, welding or cutting, undertaken as part of structural changes to the premises of ICT resources should be monitored by ICT staff, so long as there is proof of safety of new wiring required.
- 2.6.15 Clear fire instructions should be available, and in the event of fire, these instructions should be expressly followed.
- 2.6.16 Servers should be well mounted on racks and other equipment should be kept off the ground, placed on tables or desks.
- 2.6.17 The College offices should be adequately air-conditioned to provide a conducive environment for ICT equipment.
- 2.6.18 UPS should be installed as appropriate to all ICT resources.
- 2.6.19 Non-critical electrical equipment, especially high-power consumption equipment such as photocopiers, printers and kettles should not be connected to UPS sockets.
- 2.6.20 Movement of ICT equipment owned by the College should be authorised by the relevant authority in written form, and proper records should be kept for such movements.

2.7 Mobile Device Usage

- 2.7.1 Mobile devices connected to the network should adhere to the following guidelines:
 - i. Their operating system and any installed software shall be fully patched and kept up to date.
 - ii. Up-to-date antivirus and antispyware protection shall be installed to provide protection against viruses, worms, Trojan horses, disruptive programs or devices or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of the College network.
 - iii. A personal firewall shall be installed to provide protection from unauthorised intrusions.
 - iv. A mobile device shall not have a blank password and all default passwords shall be changed.
- 2.7.2 Users must take appropriate measures to protect the mobile devices against accidental loss, damage or theft.

- 2.7.3 College network and system passwords must not be stored on mobile devices unless it is a system limitation.

2.8 Anti-Virus Process

- 2.8.1 College computers and servers shall be equipped with licensed antivirus or endpoint protection software.
- 2.8.2 Any suspected computer threats or viruses should immediately be reported to the SA.
- 2.8.3 Direct disk sharing with read/write access should be avoided unless there is absolutely a business requirement to do so.
- 2.8.4 Removable media such as flash disks, external hard disk from an unknown source should always be scanned for viruses before using them.
- 2.8.5 Critical data and system configurations should be backed-up on a regular basis and data should be stored in a safe place.
- 2.8.6 When the anti-virus software is disabled, applications that could transfer a virus, such as email or file sharing should not be run.
- 2.8.7 As new viruses are discovered almost every day, the validity of antivirus software should be periodically checked.

2.9 Closed Circuit Television (CCTV) Usage

- 2.9.1 Materials or knowledge secured as a result of the use of CCTV systems shall not be used for any personal or commercial purposes unless authorised by the Deputy Principal (Administration).
- 2.9.2 Any CCTV recorded data shall only be released for use in any investigation and with the written authority from the Deputy Principal (Administration).
- 2.9.3 Daily monitoring and management of CCTV system shall be the responsibility of the Auxiliary Police or any other officer assigned to do so by the Deputy Principal (Administration).
- 2.9.4 Access to the CCTV system and stored images shall be restricted to authorised personnel only.
- 2.9.5 Users shall be granted access to the Control Room on a case-by-case basis and only and then on written authorisation from Deputy Principal (Administration).
- 2.9.6 All staff working in the CCTV control room shall be made aware of the sensitivity of handling CCTV images and recordings.

2.9.7 Any complaints about College CCTV system should be addressed to the Office of the Deputy Principal (Administration).

2.9.8 Storage and Retention of Recorded CCTV Images

- i. A retention time of 31 days shall be applicable to a major captured incident event. This is because a major incident event shall be available for investigation when needed and shall enable review of the previous video as well as of the event itself.
- ii. A retention time of 14 days shall be applicable to events which are not critical in nature or are 'one-off' incidents. This provides sufficient time for the authorities to attend the scene and retrieve the video in an event and such images and information should be deleted once the intended usage of the record is completed.
- iii. A permanent record of all major incidents which can then be provided as evidence for any subsequent investigations must be copied from the internal hard drive to a permanent storage medium such as external hard drive for a recommended retention time of one year.
- iv. The permanent record storage media should be kept by the Auxiliary Police Commander in a safe place and made available when required.
- v. The video should be exported in its native file format (i.e. without converting between formats) to maintain image quality, and no additional compression should be applied during the export process. The record should be in a format that can be read on a standard computer (e.g. Windows based) or a separate replay machine provided to which the drive can be attached.

2.10 Access Controls

2.10.1 Access control badges/cards will be issued by the Deputy Principal (Administration) and shall remain the property of the College. Where applicable, biometric gadgets may be installed for access control.

2.10.2 Users will obtain and display their access control badges/cards while in the office and where all access is controlled.

2.10.3 Users are forbidden to use access control badges/cards assigned to another person.

2.10.4 The protection of the access control badge/card is a vital responsibility for each cardholder.

- 2.10.5 Any loss of staff access card should be immediately reported to SA for immediate discontinuation of the service.
- 2.10.6 All access control transactions records shall be maintained by the Deputy Principal (Administration).

2.11 Software Use and Licensing

- 2.11.1 Only suitably licensed software may be used to perform the College business.
- 2.11.2 College's resources or networks must not be used to acquire, copy, or distribute software, or other copyrighted material without appropriate licenses.
- 2.11.3 The College reserves the rights to the applications and source codes developed on the College's ICT resources. This includes ICT applications developed and facilitated by the College.
- 2.11.4 Users shall not install College's licensed applications and software for use on non-College ICT resources.
- 2.11.5 If personal use software or media files are found to interfere with the normal operation of the College systems or are considered to pose an unacceptable risk to the College, they must be removed.
- 2.11.6 The ICT Unit shall maintain a database of properly licensed software plus records of software licenses and proof of ownership in relation to Intellectual Property Rights maintained for business purposes.
- 2.11.7 The ICT Unit shall perform periodic scans of all PCs and mobile devices to identify installed software. Instances of software identified via periodic scanning of personal computers shall be reconciled with licensing data and anomalies addressed in a timely manner. Unlicensed software shall be removed. Responsibility for such anomalies will be assumed to rest with the person to whom the PC is assigned.
- 2.11.8 Software applications that are no longer needed should be uninstalled.
- 2.11.9 Software should be used for intended purpose as stipulated in the terms and conditions of the software.
- 2.11.10 Before a user is permitted to use particular software, the designated department/unit should instruct users on the proper usage of the particular program.
- 2.11.11 The designated department/unit should inform users on the terms and conditions included in the license agreement accompanied by the program.

2.12 Technology Equipment Disposal

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmental and a legal requirement. In addition, hard drives, USB drives and other storage media store College data, some of which are considered sensitive. In order to protect the data, all storage media must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

The following guidelines shall apply for the disposal of any technological equipment:

- 2.12.1 ICT equipment such as computers, servers that have reached the end of their useful life, the ICT Unit shall securely erase all storage media in accordance with current industry best practices before disposal.
- 2.12.2 Equipment which is working, but has reached the end of its useful life shall be made available for purchase.
- 2.12.3 No warranty or support will be provided for any equipment sold.
- 2.12.4 Any equipment not in working order or remaining from the procurement process will be disposed of according to applicable environmental guidelines.
- 2.12.5 All disposed equipment must be removed from the College Asset Register.
- 2.12.6 Failure to properly dispose of technology equipment can have several negative ramifications to the College including fines and negative customer perception.

2.13 Employee Workplace Practices and User Account Termination

- 2.13.1 User account termination may arise due to employment suspension, termination, leave, retirement, death, transfer or job change.
 - i. The Directorate of AHRM should provide updated information of existing employees to the ICT Manager on a regular basis.
 - ii. The ICT Manager should act upon the updated information of employees from the Directorate of AHRM. The ICT Manager should enquire updated employees' information from the Directorate of AHRM if the information is not received on time.
 - iii. Where applicable, the Directorate of AHRM should provide information for employees who are on leave, so that their system accounts, where

necessary, can be deactivated and reactivated when they report back to office.

- iv. The ICT Manager should ensure that the system account for employees who are leaving the organisation is terminated.
- v. All ICT assets for any terminated staff should be returned to the respective department or unit.

2.13.2 The College through CERT shall conduct regular training and awareness programs for employees and students to ensure they understand safe and responsible use of ICT systems and the importance of protecting College ICT resources.

2.14 Management of Third Parties

All external organisations or individuals who wish to supply services to the College will be bound to follow these Acceptable ICT Use guidelines as part of their contractual terms. Management of third parties includes issues on third party verification, service level agreements, outsourcing, cloud computing services, equipment leasing, maintenance and support services and issues pertaining to Internet Service Providers (ISPs). In a scenario where vendors fail to deliver service as per contracts, appropriate legal action will be taken against them according to the terms and conditions stipulated in the contract.

CHAPTER THREE

IMPLEMENTATION, REVIEW AND ENFORCEMENT

3. Implementation and Review

- i. This document shall come into operation once approved by the College Governing Board.
- ii. Failure to observe these guidelines may subject individuals to loss of ICT resource access privileges, disciplinary actions or both.
- iii. This document may be reviewed from time to time on accounts of changes in the business environment of the College.
- iv. Any amendments to these guidelines shall be approved by the College Governing Board.

3.1 Roles and Responsibilities

It is the responsibility of any person using College's ICT resources to read, understand, and follow these guidelines and attached procedures and standards in the Appendix section. In addition, users are expected to exercise reasonable judgement in interpreting these guidelines and in making decisions about the use of ICT resources. Any person with questions regarding the application or meaning of statements in this guideline should seek clarifications from the Deputy Principal -Planning, Finance and Administration.

The Manager responsible for ICT shall enforce compliance with these guidelines by access revocation and removal from College systems and networks and, where applicable, to initiate disciplinary processes.

3.2 Monitoring and Evaluation

The Computer Security Incident/Emergency Response Team (CSIRT/CERT) shall be responsible for quarterly reporting the implementation and compliance of these guidelines, and recommending to the College Management through the ICT Steering Committee appropriate measures for improvement.

3.3 Enforcement

- i. The Office of the Deputy Principal- Planning, Finance and Administration shall handle all disciplinary actions related to violation of these guidelines and standard procedures in accordance with laws and regulations for third

party users and for staff through College staff rules and regulations or standing orders.

- ii. The Office of the Deputy Principal- Academic, Research and Consultancy shall handle all students' disciplinary actions related to violation of these guidelines and standard procedures in accordance with University Students rules and regulations.

4. RELATED DOCUMENTS

e-Government Act No. 10, 2019

e-Government Regulations, 2020

DUCE ICT Policy, 2025

DUCE ICT Strategy, 2025

DUCE ICT Security Policy, 2026

DUCE ICT Security Strategy Policy, 2026

DUCE Five Year Rolling Strategic Plan 2026/2027- 2030/2031

Sample Acceptable ICT Policy Use available at <https://www.ega.go.tz>

Mwongozo wa Matumizi Bora, Sahihi na Salama wa Vifaa, Data na Mifumo ya TEHAMA Serikalini, 2022

en-1773258488-Final Reviewed Creation of Government ICT Management Documents- Technical Guide- 18.2.2026 available at <https://www.ega.go.tz>

5. DOCUMENT CONTROL

VERSION	NAME	COMMENT	DATE
Ver. 2.0	Acceptable ICT Use (ICT Security) Guidelines	Develop Acceptable ICT Use	April, 2026
Ver. 1.0	ICT Security Guidelines	Develop ICT Security Guidelines	June, 2020

APPENDICES-PROCUDERES AND STANDARDS

Appendix I: Standard for Secure Passwords and Authentication Practices

1. Introduction

The purpose of this guideline is to establish standards for password creation, management, and authentication methods to protect College systems and data from unauthorised access. All Users are expected to adhere to these standards to ensure the security and integrity of our information technology environment.

2. Password Complexity Requirements

- i. Passwords must be at least eight characters in length.
- ii. Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters (e.g., !, @, #, \$, %).
- iii. Passwords must not contain easily guessable information such as usernames, personal names, or common words.
- iv. Users should avoid using the same password across multiple systems or accounts.

3. Password Management

- i. Users shall:
 - a. Change their systems passwords at most ninety (90) days, in case of any suspected breach of confidentiality, the password must be changed immediately.
 - b. Must not reuse passwords when changing passwords consecutively.
 - c. Must never share password with other individuals, including colleagues, supervisors, or ICT staff.
 - d. Must neither store password as a clear text nor written onto hard-copy surfaces, such as scratch papers, notepad, etc. Also, storing passwords in a computer file, whether on your hard drive or on flash disk, can make it accessible to unauthorised users.
 - e. Must change initial passwords that have been assigned as original user-ID passwords at the first user log-on, whether the information system forces them or not. Passwords should be chosen by the user, not by the system administrator.
 - f. Must create computer system passwords that are a minimum of eight (8) characters in length, and be comprised of letters, numbers, and special characters to the extent possible

- ii. If a password is suspected to be compromised, it must be changed immediately and reported to ICT CSIRT/CERT
- iii. Password-protected screen-savers on all PCs and servers must be implemented. The screen-savers must be automatically activated after at most five (5) minutes.
- iv. For systems that cannot have screen saver functionality, users must log off from their connection session when they plan to be away from their terminal or when they have completed their tasks.
- v. When not turned off, PCs and terminals must be protected from unauthorised use by appropriate controls, such as key-lock, BIOS password, etc.
- vi. For non-self-service forgot password change systems, users should email their request for new password to ictsupport@duce.ac.tz or <https://helpdesk.gov.go.tz>
- vii. Enforcement of Multi-Factor Authentication (MFA)
 - a. MFA shall be implemented wherever possible to strengthen system access security.
 - b. MFA requires users to provide additional verification (such as a one-time code sent to a mobile device or biometric authentication) in addition to their password.
 - c. Users must follow all instructions for enrolling in and using MFA for applicable systems and applications.

4. Enforcement

Failure to comply with these password and authentication standards may result in disciplinary action and/or loss of access privileges. Periodic audits may be conducted to ensure adherence to these requirements.

Appendix II: Software Installation and Licensing Procedures on College ICT Resources

1. Introduction

This guideline establishes the procedures and responsibilities for installing and licensing software on College Information and Communication Technology (ICT) equipment. It aims to protect the institution's digital assets including desktops, laptops, servers, and mobile devices, to ensure legal compliance, and maintain operational integrity.

2. General Principles

- i. Only authorised and properly licensed software or approved Open-Source Software may be installed on College ICT resources.
- ii. All software installations must be performed or approved by the ICT Unit
- iii. Unauthorised installation, copying, or use of software is strictly prohibited.
- iv. All software must comply with applicable copyright laws and licensing agreements.

3. Roles and Responsibilities

i. ICT Unit

- a. Evaluate, approve, and perform all software installations.
- b. Maintain records of software licenses and installation dates.
- c. Ensure compliance with licensing agreements and legal regulations.
- d. Provide guidance and support regarding software requests and usage.

ii. Users

- i. Submit software installation requests to the ICT Unit through email ictsecurity@duce.ac.tz or ictsupport@duce.ac.tz the request must have software name, version, intended use, number of licenses required, and justification.
- ii. Refrain from installing, copying, or using unauthorised software.
- iii. Report any suspected unlicensed or unauthorised software to the ICT Unit through email ictsecurity@duce.ac.tz or ictsupport@duce.ac.tz

4. Software Installation Process

- i. User identifies a need for new software and submits a request to the ICT Unit, including justification and intended use.
- ii. ICT Unit reviews the request for compatibility, necessity, and licensing compliance.

- iii. If approved, the ICT Unit will recommend for procurement of necessary licenses and perform the installation.
- iv. ICT Unit maintains a record of the installation and license information.
- v. User receives training or instructions on proper software use, if applicable.

5. License Management

- i. The ICT Unit must track all software licenses, renewal dates, and compliance requirements.
- ii. Expired or unused software licenses should be reviewed and managed appropriately.
- iii. Software audits may be conducted periodically to ensure compliance.

6. Enforcement

Violation of this procedure may result in disciplinary action, removal of unauthorised software, and/or legal consequences in accordance with College standards, regulations and other applicable laws/standards.

Appendix III: Network Security Guidelines Standards**1. Introduction**

The purpose of these Network Security Standards is to safeguard the College's information assets and technology infrastructure from unauthorised access, misuse, and cyber threats. These standards establish minimum security requirements for the configuration, operation, and management of the College's network resources. These standards apply to all College networks, including wired and wireless segments, network hardware, remote access, and all personnel responsible for managing or accessing the institution's network resources.

2. Network Security Controls**i. Firewalls**

- a. Firewalls shall be deployed at all network boundaries to filter unauthorised traffic and protect internal networks from external threats.
- b. Regularly update firewall rules shall be set to reflect current security policies and operational requirements.
- c. Restrict inbound and outbound traffic to only what is necessary for College operations.

ii. Network Monitoring

- a. Implementation of continuous network monitoring solutions to detect, log, and alert on suspicious or unauthorised activity.
- b. Retain network logs for a defined period in accordance with College policy and regulatory requirements.
- c. Conduct regular reviews of monitoring alerts and logs for signs of compromise or policy violations.

iii. Secure Configuration of Network Devices

- a. Ensure all routers, switches, and related network devices are securely configured according to industry best practices and applicable College baseline standards.
- b. Disable unused interfaces, ports, and services on all network devices.
- c. Change default passwords and use strong authentication credentials for device management.
- d. Apply security patches and firmware updates promptly as they become available.

iv. Remote Access

- a. Remote access to College systems is only permitted through approved secure channels, such as Virtual Private Networks (VPNs) that use strong encryption and multi-factor authentication (MFA).
- b. All remote connections must be logged and monitored for unauthorised access attempts.
- c. Access rights for remote users must be limited to the minimum necessary for their roles and reviewed regularly.
- d. Remote access solutions must be kept up to date and configured in accordance with standard security policies.

3. Roles and Responsibilities

- i. The undersigned network administrators in collaboration with the CSIRT/CERT Team shall be responsible for the implementation and maintenance of network security controls as defined in these standards.
- ii. All users must comply with network security requirements and report any suspected security incidents or vulnerabilities.

4. Enforcement

Failure to adhere to these Network Security Standards may result in disciplinary action in accordance to the College rules and other relevant government regulations. Additionally, individuals who do not comply may lose access privileges to College network resources.

Appendix IV: ICT Software Patching Procedure Form**1. Introduction**

This form outlines the standardized process for planning, approving, deploying, and documenting software patches within the ICT infrastructure. It aims to ensure all patches are applied consistently, securely, and with minimal disruption to business operations. This applies to all ICT-managed systems, including servers, workstations, network devices, and applications under the College control.

2. Responsibilities

- i. **ICT Administrator:** Responsible for identifying, testing, and applying software patches.
- ii. **System Owner:** Reviews and approves patch deployment schedules.
- iii. **ICT Manager:** Oversees the patch management process and ensures compliance.

3. Procedure Steps

- i. **Patch Identification**
 - a. Monitor vendor notifications, vulnerability databases, and security advisories.
 - b. Document all relevant patches for managed systems.
- ii. **Patch Assessment**
 - a. Evaluate patch criticality (security, functionality, compliance).
 - b. Assess potential impact on existing systems and applications.
- iii. **Testing**
 - a. Test patches in a controlled environment that mirrors production systems.
 - b. Document test results and any issues encountered.
- iv. **Deployment**
 - a. Schedule patch deployment during approved maintenance windows.
 - b. Notify affected users in advance.
 - c. Apply patches according to vendor instructions.
- v. **Verification**
 - a. Confirm patch installation and verify system stability.
 - b. Monitor for any post-patch issues.
- vi. **Approval**
 - a. Complete the Patch Approval section of this form.
 - b. Obtain signatures from the System Owner and ICT Manager

vii. **Documentation**

- a. Complete the Patch Deployment Log section of this form.
- b. Record any incidents, rollbacks, or deviations from the procedure.
- c. Patch Procedure Form

Date	
System/Device Name	
Operating System/Software	
Patch Name/Number	
Patch Source/Vendor	
Criticality Level (High/Medium/Low)	
Test Results	
Deployment Date & Time	
Deployment Method	
Responsible ICT Staff	
System Owner Approval	
ICT Manager Approval	
Post-Deployment Verification	
Comments/Incidents/test logs	