STANDARD OPERATING PROCEDURE		
Acceptable ICT Use Policy		Page 1 of 17
Document No: 012	Version:1.8	Relevant area: IT and all other departments

Author:

Written/Revised by: (Name, Position)	Signature:	Date:
Martin Ringia		28/1/2024

Approval cycle:

Reviewed by: (Name, Position)	Signature:	Date:
Alfred Kilamile		28/1/2024
Mangalu Masweko		28/1/2024

Authorized by: (Name, Position)	Signature:	Date:
Paul Kasanga (IBA Head) IBA Head		28/01/2024

Authorized by: (Name, Position)	Signature:	Date:
Rehema Ngamilo (COO)		28/01/2024

1. Introduction

This document formalizes the policy for employees and stakeholders ("users") of Comprehensive Community Based Rehabilitation in Tanzania, (CCBRT) on the use of information and communication technology resources; including computers, printers and other peripherals, programs, data, local area network, video conference facilities, door access control, CCTV, intranet and the Internet. In addition to this document, additional rules governing the use of specific ICT Resources may be developed, e.g., network acceptable use guidelines. Use of CCBRT's information and communication technology (ICT) Resources by any employee or third party shall constitute acceptance of the terms of this document and any such additional documents.

1.1. Purpose

This ICT policy describes the rules governing the appropriate use of ICT resources & services offered by CCBRT. It also defines how staffs are expected to utilize and maintain ICT related assets belonging to CCBRT. The policy describes three key areas namely Information, Communication and Technology and explains expected end user behavior towards utilization of related resources such as Internet, Data, Emails, Workstations (Desktops, Laptops, Thin clients) and Computer Systems.

All CCBRT ICT assets and associated data are sole property of CCBRT organization. The ICT department has been granted the role of custodian and has been mandated to carry out tasks with prior authorization. CCBRT uses technology to improve the efficiency and effectiveness of business operations throughout the organization. The ICT department thus entrusts Technology assets and resources to end users in order to facilitate smooth day to day business operations of the hospital. Therefore, this policy is meant to:

- Ensure proper utilization and maintenance of CCBRT ICT assets and resources;
- Reduce security and business-related technology risks;
- Empower staff with adequate understanding of ICT standards and expectations.

1.2. Adherence

This Standard must be adhered to by any individual who is involved in:

- Administration of CCBRT Computer Systems and Infrastructure Technology
- Making use of any CCBRT owned Technology platform and Infrastructure
- Provided with access to CCBRT Infrastructure and/or Computer Systems and assets

1.3. Non-compliance

Noncompliance to the Standard falls into one of 3 classifications: Waivers, Dispensations or Breaches.

i. **A Waiver / Deviation** excludes a function / team / dept. from the requirements of all or parts of the Standard where either they have a very low exposure to the risk that the Standard addresses; where the cost/benefit of implementing the Standard is out of balance; or where the application of the Standard would contradict local legal/ regulatory requirements in a specific country. Waivers must be agreed by the ICT Manager and must be refreshedannually.

ii. **A Dispensation** temporarily excludes a function / team / dept. from the requirements of all or parts of the Standard,pending action being taken to comply with the control requirement. Dispensations may only be granted for eithernewly acquired businesses where compliance with the Standard cannot be met, or where a new or amended Standard is issued and a business unit needs time to comply. Business units must define, execute and monitor remedial activity to address dispensations.

iii. **A Breach** is defined as an identified instance of non-compliance to all or parts of a Group Policy or supporting Standard.

- All reported cases of breaches of this Standard will be investigated and could lead to disciplinary action, upto and including dismissal for gross misconduct.

1.4. Scope

This policy applies to all staff, consultants, Interns and volunteers who make use of CCBRT ICT assets and resources. This policy is applicable for all CCBRT ICT assets and resources accessed/being used on and off CCBRT premises. It also applies to the use of any device connected to the CCBRT Technology Infrastructure or access of any CCBRT ICT resources.

1.5. Onboarding of new staff/consultant/intern/volunteer

In case of a new staff/consultant/intern/volunteer his or her respective line manager or host is expected to complete the ICT Access Request form on behalf of the individual(s) prior to their commence date. The form is to be signed by a Human Resource official before submitting it to the ICT department Service desk for further action. The new staff/consultant/intern/volunteer will be required to sign and complete an acknowledgment form once ICT access and/or resources have been provided to him/her.

In case of change in Job roles and/or office location, the staff/consultant/intern/volunteer is expected to make prior communication with the ICT department in order to facilitate the necessary changes/move.

1.6. Exit of staff/consultant/intern/volunteer

In case of staff/consultant/intern/volunteer exit, the individual is expected to comply with the Human Resource exit standard. For CCBRT Staff, an Exit form is to be filled out and signed by an ICT officer. The individual will be required to return all ICT equipment/resources initially provided. All access to CCBRT ICT assets including Emails and Computer Systems will be revoked within 24 hours of receiving exit confirmation / documentation from the Human Resource department.

2. Technology

2.1 The Internet Use

CCBRT makes internet access available to staff, consultants, interns, volunteers and guests in their discretion where relevant and useful. The internet use policy describes the rules governing internet use in CCBRT. It also sets out how authorized individuals are expected to behave when using the internet.

2.1.1 The internet use policy

- Reduces online security risk on CCBRT resources and assets;
- Informs authorized individuals of what they can or cannot do online;
- Ensures authorized individuals do not view inappropriate content at work;
- Helps CCBRT comply with legal obligation regarding internet use.

2.1.2 Policy scope

This policy applies to all staff, consultants, guests, interns and volunteers who make use of CCBRT internet as stipulated on the declaration part of IT.05 Internet Access Request Form. The policy applies to use of the internet on any device that is connected to the CCBRT network Infrastructure whether a CCBRT asset or privately owned asset.

2.3 Responsibilities

Everyone granted CCBRT internet access is responsible for using internet as stipulated in the guidelines below. All content and material viewed or accessed by the user should be appropriate as defined in this document. Users will be liable for the content and material they access using CCBRT internet service.

2.4 General internet guidelines

Internet use is encouraged when it facilitates attaining business objectives & supports company goals. For staff, interns and volunteers, this may include

- Purchase office supplies or identify suppliers
- Book business travel;
- Perform work related research.

2.4.1 Personal internet use

- CCBRT allows internet connection of one extra personal device (Mobile phone/tablet/personal laptop) per authorized individual;
- Personal internet use should be at a reasonable level and limited to the Guest network;
- All rules described in this policy apply equally to personal internet use, for instance inappropriate content is always inappropriate whether accessed for business or personal use;
- Personal internet use must not affect the internet service availability to other people in the company, for example downloading large files could cause slow access for other users.

2.4.2 Internet security

- Users must not knowingly introduce any forms of computer virus, Trojans, spyware or other malware into the company's infrastructure;
- Employees must not gain/attempt to gain access to restricted websites or systems for which they do not have authorizations either within or outside the business;
- Company data should only be uploaded to and shared via approved services. The ICT department can advise on appropriate tools for sending and sharing large amounts of data;
- Authorized individuals must not disclose their access credentials to others.
- Authorized individuals must not use or disclose other's access credentials (username and/or password).

2.4.3 Inappropriate content and uses

2.4.3.1 Users must not

- Take part in any activities on the internet that could bring CCBRT into disrepute
- Create or transmit material that might be defamatory or incur liability for CCBRT
- View, download, create or distribute any inappropriate content or material

Inappropriate contents include pornography, racial or religious slurs, gender specific comments, terrorism, information encouraging criminal skills or material relating to cults, gambling and illegal drugs;

- Use internet for any illegal or criminal activities
- Send offensive or harassing materials to others

- Broadcast unsolicited views on social, political, religious or other non-business-related matters;
- Send or post messages or materials that could damage CCBRT's image or reputation.

2.5 ICT Authority

- ICT can provide or deny permissions to various internet sites depending on requirement and necessity;
- ICT can monitor internet usage and abuse;
- ICT can provide remote VPN connection to end user when required and sees fit.
- Can revoke permission and/or access based on identified abuse.

3. e-Mail Use

CCBRT makes email services available to its employees where relevant and useful for their job function. This email use policy describes the rules governing company email account usage.

Email is a standard tool of communicating in the business. It is used widely and arguably as important as the telephone. Like any technology email can cause difficulties if used incorrectly or inappropriately. This email policy:

- Reduces security and business risk faced by CCBRT;
- Makes staff understand how they are permitted to use company email accounts;
- Ensure employees follow good email usage practices;
- Helps the company comply with legal obligations regarding email use.

3.1. Responsibilities

All users provided with CCBRT email accounts are responsible and accountable for their account activities. Users are required to adhere to proper email use as stipulated in this document.

3.2. Email Guidelines

- Always log out from your email account after use
- Use a strong password to enhance the security of your email account
- Avoid setting obvious passwords example your name, date of birth
- Routinely change your password for better security
- "Reply All" functionality should only be used when all recipients in the email chain are required to see the communication;
- The "**CC**" functionality can be used to inform any other stakeholder of the email message;
- Emails forwarding functionality can be used to avoid retyping of the message only in the case when the recipient is required to see the exact message.
- Routinely check your email account for new emails and respond at a reasonable time.
- Set an "out of office message" to communicate your absence to the sender when you are on leave/not available to respond to mail for an extended period of time.

3.3. Business email use

CCBRT recognizes that email is a key communication tool. It encourages authorized individuals to use email whenever appropriate, for instance staff may use email to:

- Communicate with other staff
- Communicate with suppliers
- Communicate with external partners and donors
- Market CCBRT services
- All individuals provided with a CCBRT email accounts are responsible for checking their emails at reasonable intervals.

3.4 Personal email use

CCBRT recognizes that email is an important tool in many people's daily lives. As such, CCBRT allows employees to use their personal email accounts with the following stipulations:

- Personal email use should be of a reasonable level. We encourage this to be during non-working hours, such as during breaks and lunch;
- All rules described in this policy apply equally to personal email use that utilize CCBRT resources, for instance inappropriate content is always inappropriate no matter if sent or received for business or personal reasons;
- Personal email use must not affect email service availability to other users, for instance sending exceptionally large files via email could slow down access for other employees.

3.5 Authorized users

Only people who have been authorized to use CCBRT emails may do so. Access is granted by the company's ICT department upon completion of ICT Access Request form (available from HR and/or ICT).

It is typically granted when a new employee joins the company. For existing employees requiring a change of email account the same procedure applies (Form is also available in the ICT Shared folder named "ICT Access Forms". Sharing of email credentials or obtaining others' credentials is strictly prohibited and may lead to disciplinary action.

3.6 Email security

Used inappropriately email can be a source of security problem in CCBRT. Users of company email system must not:

- Open email attachments from unknown sources;
- Tamper with security and email scanning software. These tools are essential to protect CCBRT from security threats;
- Access another user's company email account. If they require access to a specific message (for instance while the employee is off or sick), they should approach their line manager who in turn will communicate to the ICT department with such request;
- Users must not share email account credentials, and specifically passwords.

3.7 Inappropriate email content and use

It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances. Users must not:

- Write or send emails that might be defamatory or incur liability for the company;
- Create or distribute any inappropriate content or material via email;
- Use email for illegal or criminal activities;
- Send offensive or harassing emails to others;
- Send messages or material that could damage CCBRT's image or reputation.
- Use CCBRT email services to run commercial activities (Except as specifically offered by CCBRT management)
- Leave their email account unattended/unutilized for an extensive period of time.

3.8 ICT Authority

- ICT manages (reset/disable) end user email accounts with prior approval from authorized user or line manager.

4. Data Protection

CCBRT is a disability hospital serving a large number of patients thus gathering and storing a large amount of information, both clinical and non-clinical. This policy helps to protect the company's data resources from data security risks, including:

- Breaches of confidentiality, for instance information being given out inappropriately;
- Reputational damage, for instance the company could suffer if hackers successfully gained access to sensitive data.
- Loss of important confidential information such as patient medical records and data.

4.1.Responsibilities

All individuals provided access to data resources (users responsible for data input/processing/output) who work for or with CCBRT are responsible for ensuring that data is securely stored and handled appropriately.

These authorized individuals must ensure that organizational data is handled and processed in line with this policy and the data management standards set by the ICT department. The ICT department is the custodian of the organization's data and information systems.

4.2. Data protection guidelines

- Data access is provided to individuals on a need's basis, depending on their work function.
- Data should not be shared informally. When access to confidential information or organizational data is required, employees should obtain approval from their line manager;
- Employees should keep all data secure by taking sensible precautions and following the stipulated guidelines;
- Strong passwords must be used on Information systems and never be shared;
- Personal data should not be disclosed to unauthorized people either within the company or externally;
- Staff/consultants/volunteers/interns should request help from the ICT department if they are unsure about any aspects of data protection.
- All data, report requests should be channeled through one single source, which is the Innovation and Business Analysis unit.

4.3.Data storage

These rules describe how and where data should be safely stored. It also describes the different types of data and the steps to be taken while working with them. Further questions about storing data safety can be directed to the ICT department for guidance.

4.3.1. Organizational data

All data related to CCBRT should be stored in a secure location as advised by ICT department.

- All CCBRT data being collected by individuals working for or with CCBRT should be saved on defined logical locations such as departmental shared folders and/or individual workspace as defined and instructed by the ICT department.
- Physical files and folders should be stored in defined locations depending on the type of data they hold and should be labeled accordingly for easy and quick retrieval.
- All organizational data should be stored in a location which is being backed up to ensure there is no loss of data in case of a system failure, crush or theft.
- Sharing of CCBRT Data (such as patient data, statistics.) with 3rd party requires prior authorization from CCBRT management;

4.3.2. Personal data

CCBRT understands the need of employees having a copy of their personal data, for instance study related material, and business-related tutorials and eBooks. All personal data should be appropriate and stored at a location as advised by ICT department.

Storage of personal data is permitted on CCBRT workstations under the following stipulations:

- The data should strictly be related to your role and responsibilities towards the organization;
- All personal data should separately be stored from organizational data;
- All personal data should be of appropriate content;
- Personal data storage should not affect other users or system performance, for instance storing exceedingly large amounts of data in the wrong location.

CCBRT will not be liable for any personal data stored on organizational workstations.

4.4.ICT Authority

- ICT can grant access to organization shared folders to end user upon approval from line manager and/or folder owner;
- ICT can create new shared folders for organizational departments when required.

5.0. ICT Assets

Information Communication Technology (ICT) resources include capital assets (desktops, laptops, desk-set phones, network and power cables, printers, projectors, scanners, computer peripherals, switches, routers, servers and hubs) and software owned by CCBRT.

The purpose of this policy is to provide procedures and guidelines for usage and maintenance of ICT equipment. It is important that all authorized individuals (staff, consultants, volunteers, interns and guests entrusted with CCBRT ICT assets) are held accountable and should be responsible for the organizational ICT assets entrusted to them.

5. ICT Assets guidelines

- Keep laptops, workstations and other ICT machines away from excessive heat;
- Portable ICT assets such as Laptops and tablets must be locked when unattended.
- Properly switching off machines when not in use;

Please Note: In case machine needs to be updated then it should only be shut down when the updates are complete;

- All requests for new or change of application/system software must be presented to the ICT unit with clear user requirements as instructed by ICT
- All purchase of ICT related equipment must pass through ICT department, for instance organization software and licenses and other ICT related hardware
- Hardware and software must not be procured without consultation of ICT department
- All changes that impact or require involvement of ICT infrastructure should be discussed and approved by the Head of ICT unit
- The decision whether to upgrade software shall only be taken after consideration of the associated risks of upgrade weighed against the anticipated benefits and necessity of the change
- Do not tamper with or rearrange how equipment is plugged in (computers, printers, projectors, power supplies, network cabling, modems, etc.) without first consulting ICT department
- All CCBRT computer hardware shall be marked with an asset tag that must never be removed
- CCBRT ICT department shall identify and isolate secure areas (such as server rooms) from physical contact or access. Secure areas shall be entered only by authorized personnel
- Individuals must not tamper with or attempt to tamper with firewall and antivirus systems that are installed and maintained across the entire CCBRT network to ensure security
- Personal files, such as videos should not be saved on the Desktop, my documents or shared folder as these locations are designated for work related material only and the recycle bins should be emptied regularly
- Computers should be free from dust and water and should therefore be cleaned by a dry cloth regularly and for gate pass of ICT equipment, the ICT department must be consulted.

5.1.ICT Authority

- ICT can provide new or better ICT equipment (example; laptops, desktops, computer peripherals) to their discretion, depending on need and available budget;
- ICT can confiscate any ICT equipment in cases of abuse or misuse unless decided otherwise by management;
- ICT can carry periodic housekeeping and thus any file not related to CCBRT may be deleted and the recycle bin emptied.

5.2. Compliance and Signoff

A summarized version of the ICT Usage policy training is acknowledged in the form below, to confirm a user has well understood the definition of the dos and don'ts is also made available for review and signoff by all staff/consultant/interns/volunteers. Signing of the summarized ICT Usage Policy is a declaration of compliance and agreement to this ICT Usage policy.

Document Change Control

Date	Version	Updated by	Details
01/06/2015	1.0	Author - Shamez	Initial template
04/06/2015	1.0	Author – Edwin	Draft for Initial Review
19/06/2015	1.1	Author – Shamez and Edwin	Amendment
07/02/2018	1.2	Author – Mangalu and Edwin	Standard Review
19/02/2018	1.3	Author – Mwema and Sarah	Standard Review
17/01/2019	1.4	Author – Mwema and Edwin	Standard Review
30/12/2019	1.5	Martin Ringia	Standard Review
15/12/2020	1.5	Edwin Kashangaki	Standard Review
24/08/2022	1.6	Edwin Kashangaki	Standard Review
28/01/2024	1.7	Paul Kasanga	Standard Revisew

SOP Acknowledgement log

By signing below, I acknowledge that I have received, read and intend to follow this SOP					
		Received		Read	
Name	Role:	Signature	Date	Signature	Date