African Population and
Health Research Center

ICT POLICY

Date of Approval	November 2020
Effective Date	November 2020
Scheduled Review Date	November 2023

Table of Contents

1. Introduction

Information and Communications Technology (ICT) is used in all areas of the Center's work. In research, it is used for data collection, management, analysis and archiving; in Policy Engagement and Communications, it is used for producing communications materials, virtual interactions and extensively in social media to share and publicise our work; in Research Capacity Strengthening, it is used for virtual meetings and virtual training. In Operations, ICT underpins our finance and HR systems, and supports internal and external communications. As a result, almost all APHRC staff and other representatives will interact with ICT. Inappropriate use of ICT exposes APHRC to risks including virus attacks, compromise of network systems and services, legal issues and reputational damage. It is therefore critical to outline the acceptable use of ICT.

The ICT industry is fast paced and therefore it is important to put in place systems and processes that are up to date and in tandem with rapid changes in technology, threats, and regulatory regimes.

The APHRC ICT policy is grounded in best practice and guided by provisions in global ICT regulatory regimes such as the General Data Protection Regulation[1] and local regulatory regimes such as the Data Protection Act of Kenya[2].

2. Purpose

The purpose of this policy is to outline the acceptable use of ICT equipment and software at APHRC.

The purpose of this policy is not to impose restrictions that are contrary to APHRC's established culture of openness, trust and integrity. Rather, the ICT policy is meant to protect APHRC's employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, and FTP, are the property of APHRC. These systems are to be used for business purposes in serving the interests of the organization, our partners and stakeholders.

3. Scope

This policy applies to employees, contractors, consultants, and temporary staff at APHRC, including all personnel affiliated with third parties. This policy applies to all ICT equipment that is owned or leased by APHRC.

4. General Use and Ownership

a) While APHRC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

property of APHRC. Because of the need to protect APHRC's network, management can access all the information stored on any network device belonging to APHRC e.g. PCs, laptops, Mobile phones, Tablets and PDAs. Where necessary, management will access this information.

b) Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The ICT departments is responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, and if there is any uncertainty, employees should consult the ICT Manager.

c) Any information that users consider sensitive or vulnerable should be encrypted. Staff handling sensitive or highly confidential information will be trained by ICT on how to encrypt files.

d) For security and network maintenance purposes, authorized individuals within APHRC may monitor equipment, systems, and network traffic at any time.

e) APHRC reserves the right to audit networks and systems periodically, to ensure compliance with this policy.

5. ICT Equipment

Acquisition

a) The ICT Department shall establish and update annually, a list of standard hardware, peripherals and software approved for purchase with APHRC funds and/or supported by APHRC technology resources.

b) ICT department will ensure that hardware is acquired from authorized brand dealers who provide the necessary warranties.

c) ICT recommendation and management approval should be sought where unique hardware equipment is necessary for specialized work. Decisions on the specialized equipment to be procured will be based on technical considerations rather than personal preferences.

d) All equipment valued at more than USD 400 should be comprehensively insured within 24 hours of acquisition. To enhance this process, the ICT department will provide the Finance department with the delivery note and invoice within 12 hours of delivery.

Handling

a) All equipment should be handled with care. Users will be held liable for any malfunction or breakage resulting from their negligence excluding normal wear and tear. Users will also be held liable for equipment lost or stolen as a result of negligence. Negligence here is simply defined as a failure to act with the prudence that a reasonable person would exercise under the same circumstances.

b) It is the user’s responsibility to ensure that all accessories that accompany the equipment (e.g. chargers, power banks, earphones, covers etc) are well maintained and returned in the same condition as they were acquired. Any costs incurred to repair or replace the equipment's accessories will be directed to the assigned user.

c) Non-portable ICT equipment should always remain in designated locations. Relocation will only be done with prior approval and/or involvement of the ICT department.

Security

a) APHRC shall provide appropriate security measures for its equipment.
b) Users shall ensure that provided security measures are utilized and up to date at all times. Failure to use these measures will amount to negligence.
c) Access to the server room is restricted to authorized ICT personnel only and the Director responsible for the ICT unit. All other staff and/or contractors will require an escort anytime access is required and a log recorded by the accompanying ICT staff. The ICT staff providing escort must remain in the server room until the individual requiring escort exits the server room.
d) The server room door must remain closed and locked at all times.

Disposal

a) Computers are expected to be used for a minimum of three years from acquisition before replacement or disposal. Other hand held ICT devices may last less than three years while heavy equipment like bulk printers remain in economic use for more than three years and are depreciated accordingly as per the Center's *Finance Policy*. In the event that a computer or device still meets the needs of the user, and subject to ICT assessment and diagnosis, a longer retention period might be considered.
b) ICT equipment will be disposed of using procedures described in the *APHRC Disposal Manual.*

Usage

a) All APHRC equipment will be used solely for official purposes.
b) Personal computers or equipment will only be used to conduct APHRC related business with the approval of the ICT department.

6. Software

Installation and configuration

a) Only authorized and licensed software should be installed on APHRC equipment.
b) All installations must only be done by authorized ICT personnel
c) Installation of personally licensed and genuine software will only be authorized for use in an APHRC ICT environment or computer with the approval of the ICT department
d) APHRC licensed software will not be installed in personal equipment that has not been authorized for usage to conduct APHRC work.

Security

a) Sharing APHRC owned ICT equipment issued to staff is strictly prohibited.
b) Sharing of user IDs and passwords is strictly prohibited

c) Anti-virus software will be provided for all ICT equipment owned by APHRC requiring the software.
d) Access rights and permission to centralized software and databases will be assigned according to the level of use.
e) External computers or equipment not owned by APHRC must meet the minimum security measures set by the ICT unit as below: Genuine operating system
    - Genuine and up to date antivirus
    - Have a sponsor from APHRC
f) All APHRC passwords must be changed after every three months.
g) All APHRC passwords must meet the below criteria:
    - Must contain a minimum of 8 characters
    - Must contain at least one number
    - Must contain at least one special character
    - Must contain at least one capital letter

7. Intellectual Property

Software, databases, and other tools internally developed for use at APHRC will be the sole property of APHRC. Usage outside APHRC is strictly prohibited unless authorized by management.

8. Internet, Email and Related Services

Internet

a) Internet and related services will generally be used for APHRC related work.
b) APHRC reserves the right to restrict access to any site that is considered inappropriate for APHRC operations.
c) Staff are prohibited from downloading and/or viewing content of an inappropriate nature, or which incites violence/untoward behaviour. This extends also to downloading content that may infringe on other people's copyright.
d) A record is maintained of sites visited and extent of use. The ICT department will notify management of excess or inappropriate use for disciplinary action to be taken as appropriate in line with the Center's policies outlines in the *HR Policies and Procedures Manual.*
e) Visitors will be issued with temporary login details to access the Internet upon request from an APHRC staff member (sponsor). A request should be made at least three days before the visitor arrives and a week in advance for big groups of more than five individuals. Access to any ICT resource by external users is prohibited and will be monitored using the ICT control structures already put in place via the Network Access Controller.

E-Mail

a) Email account passwords must be changed every three months.
b) APHRC designated E-Mail accounts will generally be used only for APHRC related work.
c) APHRC HR department can authorize access to an active or past APHRC individual staff email communication (inbox) for official use or reference.
d) Sending and forwarding of inappropriate emails is prohibited
e) Sharing of designated e-mail accounts is prohibited. The only exception to this rule will be for the Executive Assistants working with the Directors or program heads. Such shared access will be done with the knowledge of the ICT department.
f) Employees must exercise the utmost caution when sending any email from APHRC account to an outside network. Unless appropriate authorization has been obtained, APHRC email should not be automatically forwarded to any external destination. This is in line with the prevailing national and international laws governing data privacy, protection and use; General Data Protection Regulation[3] and Data Protection Act of Kenya[4].
g) All users shall abide by the email etiquette that guides email correspondence between various parties, storage and archiving of emails among others. The ICT department will from time to time issue guidelines on the same.

Intranet

a) Posting of offensive and inappropriate material on the intranet is prohibited.
b) The information posted on the intranet is for internal use only and can only be accessed by staff.

Network and Telephone

a) Only authorized equipment may be used within the APHRC network.
b) Domain passwords must be changed every three months.
c) Management reserves the right to deny access to the APHRC network.
d) Access to APHRC network with devices not owned by APHRC must be approved by the IT unit as outlined in the ICT Guidelines and Procedures document.

Back-up

a) A copy all APHRC related data and documents (stored in drive D) must always be saved in the server for the purpose of backing up.
b) All backups must be saved in the cloud daily.
c) Backup restoration exercise should be done on a biannual basis to test recoverability and the integrity of data in case of a disaster in line with the Business Continuity and Disaster Recovery plan.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[4] http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

9. Roles and Responsibilities

All staff, employees, consultants and entities working on behalf of APHRC are responsible for enforcing this policy. Effective ICT security is a team effort involving the participation and support of every APHRC employee and affiliate who deals with information and/or information systems. It is the responsibility of every user to familiarize themselves with this policy and to conduct their activities accordingly

Details on the specific roles of various staff, functions including the ICT manager and the ICT committee are contained in the ICT Procedures Guidelines. In addition, the following individuals have roles and responsibilities as outlined below:

The Board of directors is responsible for the review and monitoring implementation of the policy

Executive Leadership Team (ELT)

APHRCs ELT holds overall responsibility for this policy and its implementation. They shall:

- Ensure that the Center's has quality hardware, software and robust ICT systems.
- Continuously communicate with staff about the Center's stance on this policy
- Promptly deal with any concerns reported about this policy
- Approve any external use of internally developed software, databases and other ICT tools

10. Non-compliance

Any employee found to have violated this policy may be subjected to disciplinary action, including termination of employment as outlined in the *HR Policies and Procedures manual*.

11. Monitoring and Review

The Internal Audit Unit and the ICT Committee will monitor the implementation of this policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be captured in every three years review or earlier where needed.

12. Related Policies

i. Finance Policy-outlines the insurance requirements for ICT equipment and the depreciation procedures
ii. HR Policies and Procedures manual – outlines disciplinary measures for breach of policy
iii. ICT Procedures and Guidelines – outlines roles and responsibilities of individuals and functions within APHRC
iv. Whistle Blowing Policy – describes reporting procedures and channels
v. APHRC Disposal Manual – describes procedures for disposal of equipment
vi. Business Continuity and Disaster Recovery plan – outline back up testing and recovery procedures for data

AFRICAN POPULATION AND HEALTH RESEARCH CENTER (APHRC) Policy on ICT

I, _____(Employee's Name), have received a copy of the ICT policy dated September 2020. I have read and understood it and agree to adhere, at all times, to the stipulated terms. I acknowledge that this policy is a contract of employment.
I also understand that I shall be subjected to the stipulated consequences, if I fail to adhere to the terms.

Signed: _____ Date: _____
(Employee Signature)