Kenya Water Institute
Training, Consultancy and Research in the Water Sector

KENYA WATER INSTITUTE (KEWI)

MIT DEPARTMENT

INFORMATION TECHNOLOGY & COMMUNICATION POLICY

EFFECTIVE 2016

Table of Contents

PREFACE 3
1.0 Introduction 4
a) Definitions and Terms 4
c) Objectives 4
d) Responsibilities of Users 5
2.0 ICT Security 7
3.0 Network Access & Permissions 7
4.0 Website(s) 8
5.0 ICT Equipment Maintenance. 8
6.0 Email Usage 9
7.0 Internal ICT Support 9
8.0 The Internet 9
9.0 Out-Sourced ICT services 10
10.0 ICT Staffing 10
11.0 Acquisition and Disposal of ICT Facilities 10
12.0 Backup & Disaster Recovery 11
13.0 Printers, Telephone Lines, Fax, Scanners and Copiers 12
14.0 ICT Training 12
15.0 Enforcement and Control 13
16.0 Privacy and Confidentiality 13
17.0 Revision 13

PREFACE

In order to protect our network, computers and the confidential data, KEWI has instituted this Information Systems and Network Policy.

This policy and the guidelines herein, set forth conditions for the use of information technology resources, including the Institute network equipment, access to outside networks through the local network, software, and digital media. We're protecting against not just the damages and liability created when unauthorized access occurs, but also against viruses and physical damage to our systems.

Therefore, all members of the Institute community must use all Institute computing and information resources and services in a manner that respects and maintains the public trust.

Endeavors have been made to keep the document simple to understand, to guide system administrators and users of these systems.

Employees are advised to contact the head of Information Technology whenever they are in difficulty and in need of advice, elaboration, definition or explanation for matters pertaining computer use.

This ICT Policy has been developed, in consultation with various experts in Information systems and with comparative references, to the ICT Board Laws and the General Kenyan Laws applicable to allow it become a legal document for the Management of systems in the Kenya Water Institute.

KEWI Campuses

The policy also covers all KEWI Campuses. These will be supported from the KEWI Nairobi campus.

1.0 Introduction

This document sets forth standards which must be adhered to by all Users, contractors and any user granted access to any machine on the LAN at any time, whether physically present at the Institute or via remote access.

Failure to comply with the policies set forth in this document will result in disciplinary action, and may result in termination of employment.

a) Definitions and Terms

For the purposes of this document, a "User" is any user, employee, student, contractor, agent, temporary worker, vendor and any other person in a position to know or obtain information about computers or devices on the Local area Network (LAN).

The “Firewall” is a hardware or software device which protects the ports of computers on the LAN. For the purposes of this document, "Remote Access" shall mean access to the Local Area Network from any location outside the firewall by any method.

Other terms:

CD – Compact Disk
Head of ICT – Director ICT
DRS –Disaster Recovery Site
DVD – Digital Video Disk
ICT – Information and Communication Technology
ISO – International Organization of Standards
IT – Information Technology
KEWI – Kenya Water Institute
LAN – Local Area Network
PABX – Private Automatic Branch Exchange
PC – Personal Computers
SAN –Storage Area Network
SLA – Service Level Agreement
WAN – Wide Area Network

c) Objectives

- Ensure provision of adequate and reliable information systems
- Provide guidelines on the usage of ICT software, hardware and services
- Promote efficient utilization of ERP system for improved transaction processing and more accurate data entry and reporting.
- Ensure information security and enhance continuity of operations in the event of a disaster through regular backups.

- Continue to utilize cost-effective training methods to ensure the full use of existing information technology capabilities by institute students as well as by employees.
- Expand training opportunities that enable employees to update current technical knowledge and skills as the commercially available information technology tools that they rely upon are updated.
- Ensure that the IT management systems keep pace with future requirements and technology.

d) Responsibilities of Users

1. A user shall use the Institute computer resources responsibly, respecting the needs of other computer users.

2. A user is responsible for any usage of his or her computer account, computing resources or data entrusted to him or her. Users should maintain the secrecy of their password(s).

3. A user must report any misuse of computer resources or violations of this Policy to their department head or to the Head of ICT.

4. A user must comply with all reasonable requests and instructions from the computer system operator/administrator.

5. When communicating with others via the Institute computer system, a user's communications should reflect high ethical standards, mutual respect and civility.

6. Users are responsible for obtaining and adhering to relevant network acceptable use policies including the Information Resources Security Policy and the Network Connections Policy.

e) Scope

The Policy applies to any person granted authorization to access any ICT device/facility/service on the Institute's LAN/WAN (an "Authorized User"). This includes but is not limited to contractors, temporary workers, vendors, sub-contractors and partners authorized to access any of the Institute's computers, locally or via Remote Access, for any reason, including email and Internet or intranet web browsing.
These are:

Facilities

i. Computer labs
ii. Server room(s)
iii. ICT maintenance room
iv. All ICT facilities installed at KEWI

Services

i. Provision of guidance and expertise training on ICT
ii. ICT support in software, hardware and any other computing infrastructure
iii. Technical support to staff and students

Hardware

i. PCs
ii. Laptops
iii. Tablets
iv. Printers
v. Scanners
vi. Servers
vii. Network routers, switches and Network Devices
viii. Power backup equipment (e.g. Uninterruptable Power Backup - UPS)
ix. LCD Projectors
x. Digital Cameras and Camcorders
xi. PDAs, Smart phones and other Mobile Computing Devices
xii. Flash-disks/external hard-disks/Diskettes/CDs/DVDs
xiii. PABXs, Telephone heads, fax and photocopiers
xiv. All other ICT related hardware

Software

i. Network operating systems
ii. PC operating systems
iii. Application software
iv. Utility software
v. ERP, GIS, Exchange server
vi. KEWI website

2.0 ICT Security

a) All KEWI systems and information shall be effectively protected against unauthorized access.
b) The Systems Administrator shall provide network service to staff to transmit data to requesters and store data files in an authenticated central server.
c) Users within same directorate/working group will be given access level that allows them access to their files/folders.
d) For traceability and identification, all hardware shall be barcoded and included in the KEWI asset register. This shall include any hardware bought for /donated to KEWI by external agencies.
e) ICT devices are susceptible to theft and unauthorized access, thus, strong security measure to safeguard them shall be provided.
f) Portable or laptop computers shall not be left unattended in public places, and shall be carried as hand luggage for security.
g) Portable computing equipment for short term lending shall be stored in secure lockable cabinets.
h) An updated register of all ICT equipment e.g. LCD projectors loaned out to authorized personnel shall be maintained.
i) All data storage media shall be stored in secure environments that meet manufacturer's specifications for temperature and humidity.
j) Hard copies of systems documentation shall be physically secured in filing cabinets when not in use.
k) It is the responsibility of respective users of any non LAN connected and official computing equipment (especially laptops/notebooks) to arrange with the ICT support for installation of antivirus software and to perform periodic (at most every fortnight) updates to the antivirus.
l) All ICT hardware or software will not be taken off-site from KEWI offices, for serving and /or upgrading without written authority from Head of ICT.

3.0 Network Access & Permissions

a) Each user will have only one personal identification code (User ID/user name and password) with necessary access levels and privileges.
b) User IDs will be consistent in structure i.e. the fist letter of the first name and last name, all in lower cases (ignoring middle names). If this combination conflicts with another user, then the first letter of second name will be used as the second letter of the user ID. If the officer does not have other names, then letter ‘a’ through ‘z’ will be used so that user ID is unique within KEWI access systems.

c) All devices will require access credentials (user ID and password) to be accessed over the network. Guidelines on structure of user IDs and passwords will be provided by Head of ICT.
d) Users will be responsible for the confidentiality of their access credentials and prevention of any unauthorized access to ICT equipment. Any attempt to use other users' credentials to gain access to network resources is strictly disallowed. Any account found to be compromised or shared shall be discontinued and a new one issued where necessary.
e) Only authorized personnel are allowed access to ICT resources.
f) Access credentials shall immediately be deactivated and confirmed in a clearance certificate by the Head of ICT once a member of staff ceases to be an employee of the Institute.
g) Head of ICT is authorized to gain access to a user account and folders if that account is suspected to have breached systems security or is in violation of this policy.
h) The Systems Administrator shall enforce standardization of systems and network configuration, including directory structures, to simplify network management.

4.0 Website

a) The Institute shall ensure that the KEWI Website is kept in an updated status at all times. By use of the latest technology, the website shall be maintained in a user friendly and accessible state.
b) All requests for changes on the website shall be subject to the approval of the KEWI ICT committee that shall comprise of representatives of the Institute:
    - ✓ Accounting/Authorized Officer - Chair
    - ✓ Head of ICT Unit – Secretary
    - ✓ Representative from key directorates/departments/units
    - ✓ Public Relations Officer (PRO)
    - ✓ Legal Officer
c) The Systems Administrator shall ensure that the website is always available to the public.

5.0 ICT Equipment Maintenance.

a) The Head of ICT shall ensure that all ICT equipment is kept in proper working condition at all times.
b) All ICT equipment shall be maintained in accordance with the procedure for ICT equipment maintenance.
c) In areas where the Institute has no adequate internal capacity, annual maintenance contracts will be entered into with service providers.

6.0 Email Usage

a) Staff shall be issued with official standardized e-mail addresses
b) All official email communications shall be through official email addresses. Head of ICT will ensure that mail service is available to staff always.
c) The KEWI's Intranet will be used to communicate all relatively static information (e.g. policies, procedures, briefing documents, reference material and other standing information).
d) Email users shall avoid broadcast communication (i.e. send to large groups of people using email aliases) unless where absolutely necessary. One must always ensure proper audience segregation is used before sending an email.
e) KEWI mail service shall not be used to broadcast other unofficial information or requests (e.g. information or opinions on political matters, social matters, and personal requests for information etc.)
f) Emails with attachments greater than 10MB will require authorization from Head of ICT. This will remove unnecessary load on the network and the mail server so as to guarantee equitable bandwidth sharing by all staff.

7.0 Internal ICT Support

a) While KEWI will strive to provide ICT support services, officers assigned to hardware must ensure they are not exposed to risks that can cause their damage.
b) ICT officers will be available to offer technical support on any software or hardware upon users' requests.
c) Where applicable, equipment to be used out of office shall be accompanied by an ICT Technician to ensure proper packaging, offloading and installation at destination.

8.0 The Internet

a) All connections to the Internet within KEWI offices shall be implemented through the KEWI Internet connections via a firewall.
b) To protect KEWI systems from Internet attacks or denial of service by Internet malware, all software downloads shall be authorized by Head of ICT. Such a download will be passed on to the requester only if it passes the ICT security tests and if it is permitted for free use by its manufacturers.
c) No copyright material shall be downloaded from the internet or utilized in breach of its license agreement.
d) Internet services shall be provided only through the KEWI Internet connection or KEWI USB modems or any other approved gadgets.

e) To optimize internet bandwidth usage, Institute's network shall not be used to stream music and video as these lead to deprivation of the same capacity to legitimate users during normal working hours except, where such permission is granted by Head of ICT in writing.
f) KEWI internet and network resources shall not be used to access or transfer any material containing:
    i. Derogatory remarks based on race, religion, gender, physical disability or sexual preference.
    ii. Images or references that may be considered to be offensive or in breach of any law or regulation.

9.0 Out-Sourced ICT services

a) The Institute shall out-source ICT Equipment and/or services whenever such capacity lacks in the Institute with approval from the Director upon recommendation from Head of ICT. Such a need shall be supported by a needs assessment report from Head of ICT.
b) Acquisition of such services will be guided by the Public Procurement and Disposal Act (PPDA),2005, and Public Procurement and Disposal Regulations (PPDR), 2006.
c) All out-sourced ICT equipment and services will be supervised by Head of ICT in accordance with Service Level Agreements (SLAs) that are signed in consultation with Head of ICT.
d) The out-sourced services shall be based on annual contracts that may be renewed based on recommendations from the Head of ICT.

10.0 ICT Staffing

a) The Institute commits to equip and maintain adequate and highly skilled ICT personnel for guaranteed minimum acceptable ICT service level.
b) The ICT function will be executed through the Systems Administrator headed by Head of ICT.

11.0 Acquisition and Disposal of ICT Facilities

a) Acquisition of ICT Facilities

a) Acquisition of ICT facilities shall be guided by the Public Procurement Procedures and Guidelines in the Public Procurement and Disposal Act (PPDA), 2005, Public Procurement and Disposal Regulations(PPDR)2006, Best Practices and the KEWI Procurement Manual. Where funds are donated from external sources, the

respective donor conditionalities, terms, agreements or memoranda of understanding shall apply.

b) All User requests for acquisition of items of ICT nature shall be channeled through the Head of ICT who will confirm lack or availability of such items in the Institute. If not available, Head of ICT will prepare specifications in consultation with the requesting Department and forward the request to the Director for approval.
c) In order to minimize the costs, KEWI will standardize software and hardware to be used within the Institute with advice from Head of ICT. This will be reviewed annually as need arises.
d) All Heads of Departments will forward to Head of ICT their software and /or systems needs who will offer technical guidance and support in facilitating the acquisition process.
e) ICT goods, related services and/or works once acquired will be received by the Institute's Inspection and Acceptance Committee in line with The Public Procurement and Disposal Act (PPDA), 2005 and Public Procurement and Disposal Regulations (PPDR), 2006 framework. The Committee shall seek professional assistance from Head of ICT.
f) The Systems Administrator shall ensure that all software licenses in use in the Institute are promptly renewed to guarantee smooth Institute operations and continuous software updates and support from manufacturers.
g) The Institute will strive to maintain reliable hardware infrastructure by upgrading aging ICT equipment every three years.
h) In order to avail adequate and reliable computing capacity to the technical staff, the Institute shall provide at least one functional computer to every technical staff both at the headquarters and at the campuses.

b) Disposal

a) Head of ICT shall identify hardware and software to be disposed and liaise with Procurement Department for assessment leading to disposal as per PPDA, 2005 and the PPDR, 2006.
b) Head of ICT shall ensure that all equipment earmarked for disposal are cleared of Institute data and software.

12.0 Backup & Disaster Recovery

a) KEWI' information resources such as data, business contacts, emails, text documents, presentations, contracts, accounts and other valuable information shall be safely preserved in a recoverable state.

b) Systems Administrator will maintain consistent automated backup mechanisms to preserve KEWI data in a distributed Storage Area Network (SAN) and at a DRS in order to ensure data recovery in the event of accidental loss.
c) All KEWI data shall be saved in organized shared folders in allocated campus servers from where they will be backed up in SAN and Disaster Recovery Site (DRS) through synchronized mechanism in addition to tapes or external drives in accordance with the KEWI Backup Plan.
d) Network and server administrators will ensure data is copied to these allocated servers and in all other backup destinations.
e) It is the responsibility of the respective users of any non LAN connected computing equipment (including laptops/notebooks) to arrange with the server administrator for the transfer of official data from these non LAN-connected equipment to the relevant server folders every day where practical.
f) Any unofficial files shall not be allowed on KEWI Servers.
g) To implement an ICT seamless backup service, all officers connected to KEWI LAN shall login to centralized authentication servers. Officers working from remote locations will be required to dock to the KEWI network to back up official data.

13.0 Printers, Telephone Lines, Fax, Scanners and Copiers

a) KEWI Staff are expected to use the above peripheral devices responsibly. Irresponsible or usage of these facilities for personal gain is prohibited, and may lead to denial of the service and/or surcharge.
b) Where possible, users are required to print on both sides of the paper. ICT support team will give guidance on how various printers are able to print both sides.
c) Printers will be configured to be shared by many users and placed in secured open offices where possible.
d) Unofficial calls and fax will be charged on the user.
e) An electronic document scanner shall be used to minimize usage of fax machines, printers and copiers, saved in suitable formats and emailed to recipients.

14.0 ICT Training

a) Institute's ICT training needs shall be assessed by the Head of ICT and recommendations captured in the Institute's training plan.
b) The Head of ICT shall recommend ICT trainings relevant for every section and forward requirements to Human Resources and Administration.
c) KEWI staff will be trained on emerging technologies as the Institute may determine from time to time in consultation with Head of ICT.

15.0 Enforcement and Control

a) Deliberate breach of this policy statement may lead to disciplinary measures in accordance with KEWI Human Resource Manual.
b) These may include but not limited to the offender being denied access to computing facilities or surcharge for the loss or abuse of ICT facility or service.
c) Whenever surcharge is imposed on negligence as noted in (a) above, due process will be followed in imposing the surcharge.
d) Unauthorized access to information, facility or computer (including workstations and PCs), over network or to modify its contents is strictly forbidden.
e) Officers within KEWI network shall not write, publish, browse, bookmark, access or download obscene, pornographic or pedophilia materials.
f) All hardware, software and /or systems in use in KEWI stations shall be licensed. Any officer using unlicensed products shall bear legal consequences for the product as per 'the Copyright Act, 2001'.

16.0 Privacy and Confidentiality

a) The Institute shall guarantee right to privacy and confidentiality of individual staff information while discharging ICT services.
b) Information/services/resources available within IT facilities will not be used to monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Without limitation to this provision, the following shall be excluded:
    i. In the case of a specific allegation of misconduct or for any other investigation purpose, the Director may authorize access to such information or denial of service while the staff is under investigation.
    ii. Where the Systems Administrator or any other Institute section cannot avoid accessing such information whilst administering, resolving ICT systems problems or in their day to day work activities.

17.0 Revision

This ICT Policy is applicable to the KEWI staff and students and will be updated every three years to reflect the emerging changes in the Institute, statutory regulations or for any other purposes as may be advised from time to time by Head of ICT

Where clarification of any regulation contained in this manual is required it should be sought from the Director, Kenya Water Institute.

Approved by the Governing Council for Implementation

……

Dr. Leunita A. Sumba

DIRECTOR/SECRETARY TO THE GOVERNING COUNCIL

FOR: THE GOVERNING COUNCIL

DATED: MARCH 2016