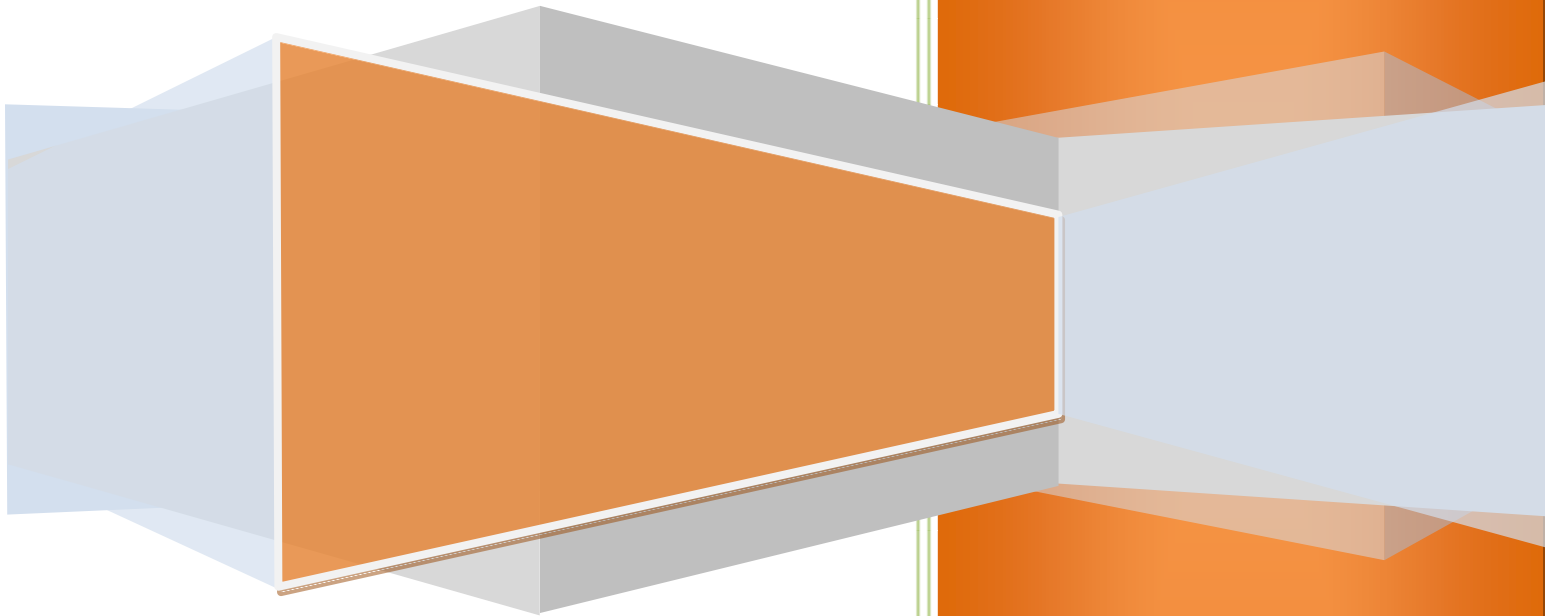


2008



Information Communication Technology(ICT) Policy



Prepared By: KenGen ICT Policy Team



TABLE OF CONTENTS

1.0. Preamble.....	3
2.0. Objectives	3
3.0. Scope	4
4.0. Precautionary and Disciplinary Measures	4
5.0. Email Policy	6
5.1 When to use email:	6
5.2 Use of Distribution Lists:	7
5.3 General points on email use:.....	8
5.4 Email etiquette:	9
5.5 Delivery & Receipt of Mails	10
6.0. Internet Policy	11
7.0 Network Security And Access Policy	12
8.0 Data Centre and DRC Access Policy	13
9.0. Policy on Printers, Telephone lines, fax and Copiers....	13
10.0. Policy on Passwords	13
11.0. Policy on ICT Related Training.....	14
12.0. Policy on Online Subscriptions.....	15
13.0 Policy on ICT Disaster Recovery	15
14.0 Policy on ICT Technical Assistance Request & Complaints.	15
15.0. Miscellaneous	16
16.0. Revision.....	17
NOTES	18
APPROVAL	20
ABBREVIATIONS	21

1.0. Preamble

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. KenGen is not an exception. While the board and the management of KenGen recognize this fact, organizations all over the world, including KenGen, are faced with the challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance. This ICT Policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by both KenGen employees and KenGen business partners.

2.0. Objectives

All KenGen's ICT facilities and information resources remain the property of KenGen and not of particular individuals, teams or departments (Note 1). It is in view of this fact that the objectives of this document are thus to:

- enhance compliance with the laws of Kenya.
- enhance information security of KenGen systems.
- enhance best practice according to ISO.
- enhance efficient use of information systems by KenGen employees and the affiliates.
- enhance availability of ICT systems
- enhance a spirit of awareness, co-operation, trust and consideration for others.

3.0. Scope

The ICT policy document relates to all Information Technology facilities and services provided by KenGen including, but not limited to, email system, databases, SAP, operating systems(windows and unix) , internet, telephone systems, wireless communication, printers and copiers. All KenGen employees, volunteers as well as business partners are expected to adhere to it. The document shall be effective from the date of approval.

4.0. Precautionary and Disciplinary Measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computing facilities.

4.1 Copyright:

Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements.

Copying software for use outside these agreements is illegal and may result in criminal charges.

4.2 Security:

4.2.1 Don't attempt to gain unauthorised access to information or facilities. It is an offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you don't have access to information resources you feel you need, contact your IT Support person or provider through the helpdesk system.

4.2.2 Don't disclose personal system passwords or other security details to other staff, volunteers or external agents and don't use

anyone else's login; this compromises the security of KenGen. If someone else gets to know your password, ensure you change it or get IT Support to help you (Note 2).

4.2.3 If you leave your PC unattended without logging off or locking the session, you are responsible for any misuse of it while you're away.

4.2.4 ALWAYS check floppy disks and flash disks for viruses, even if you think they are clean (Contact IT support for help). Computer viruses are capable of destroying KenGen's information resources. It is better to be safe than sorry.

4.3 Information about people: If you're recording or obtaining information about individuals make sure you are not breaking Data Protection legislation (your Manager can guide you on this).

4.4 You are a representative of KenGen when you're on the Internet using email:

4.4.1 Make sure your actions are in the interest (and spirit) of KenGen and don't leave KenGen open to legal action (e.g. libel).

4.4.2 Avoid trading insults with other people using the Internet with whom you disagree.

4.4.3 Obscenities/Pornography: Don't write it, publish it, look for it, bookmark it, access it or download it.

4.5 Electronic Espionage: Any information available within IT facilities must 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. Exceptions are:

i) In the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation. This may necessitate disabling the victim from accessing IT facilities pending investigation.

ii) When the IT Support section cannot avoid accessing such information whilst fixing a problem. The person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.

iii) Systems administrators, database administrators and auditors in their day to day work activities.

5.0. Email Policy

5.1 When to use email:

5.1.1 Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or paper memo).

5.1.2 Use the phone (including voicemail if no reply) for urgent messages (email is a good backup in such instances).

5.1.3 Use KenGen's intranet (not email) to communicate all

relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information). Record information on the intranet in a well structured manner, (consulting with the Web Systems Administrator as appropriate). Use email merely as a pointer to draw attention to new and changed information on the intranet.

5.2 Use of Distribution Lists:

5.2.1 Only send Email to those it is meant for; don't broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer and network performance and wastes disc space.

5.2.2 Use the standard aliases (Note 3) for work related communication only.

5.2.3 If you wish to broadcast other non work related information or requests (e.g. information or opinions on political matters outside the scope of KenGen's campaigning, social matters, personal requests for information etc.) it is better to use a Webmail account (Note 4) or a personal email account at home; don't use the standard (work) aliases.

5.2.4 Keep KenGen's internal email aliases internal. If you are sending an email both to a KenGen alias and outside of KenGen, use the alias as a blind carbon copy (i.e. the bcc address option) so that the external recipient does not see the internal alias.

5.2.5 Don't broadcast emails with attachments to large groups of people - either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

5.3 General points on email use:

5.3.1 When publishing or transmitting information externally be aware that you are representing KenGen and could be seen as speaking on KenGen's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

5.3.2 Check your inbox/in-tray at regular intervals during the working day. Keep your in-tray fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

5.3.3 Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.

5.3.4 Use prefixes in the subject box whenever appropriate (Note 5).

5.3.5 Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicise their displeasure at the actions / decisions of a colleague).

5.3.6 Don't forward emails warning about viruses (they are invariably hoaxes and systems administrators will probably already

be aware of genuine viruses - if in doubt, contact them for advice).
Exception: Only Systems administrators can forward warnings about viruses.

5.4 Email etiquette:

5.4.1 Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are also copying another group of people.

5.4.2 Make your subject headers clear and relevant to your reader(s) e.g. don't use subject headers like "stuff" Don't send a subject header of, say "accounts" to the accountant

5.4.3 Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.

5.4.4 Using asterisks at each end of a word (eg *now*) is common practice for highlighting text.

5.4.5 Capitals (eg NOW) can also be used to emphasize words, but should be used sparingly as it commonly perceived as 'shouting'.

5.4.6 Don't open email unless you have a reasonably good expectation of what it contains and the source of the mail, e.g. Do open report.doc from an Internet colleague you know, Don't open

explore.zip sent from an address you've never heard of, however tempting. Alert IT Support if you are sent anything like this unsolicited. This is one of the most effective means of protecting KenGen against email virus attacks.

5.4.7 Keep email signatures short.

Your name, title, phone/fax and web site address may constitute a typical signature.

5.4.8 Understand how forwarding an email works.

If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope).

If you forward mail *and edit it* in the process, it appears to come from you - with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope).

5.5 Delivery & Receipt of Mails

The nature of email is very controversial, as while a certain mail may be SPAM to one person it may not be SPAM to another. There are lots of SPAM filtering software out in the market, but none is perfect. There are always cases of some mails being passed out by the software as being clean while it is not clean (*false positives*) or being rejected as SPAM while it is not SPAM (*false negatives*). This controversy is further complicated by the fact that there are many

parties involved in a mail. For a mail to be successfully delivered it entails that:

1. The sender uses the correct address.
2. The internet of the sender is up.
3. The internet of the recipient is up.
4. That the sender's organization server has no technical problems.
5. That the recipient's organization mail server has no technical problems.
6. That the sender's PC is online.
7. That the recipient's PC is online.
8. That the anti-spam software recognizes it appropriately.

It is due to this complexity that, urgent mails should be given at least 15 minutes for delivery and followed up through telephone. Users receiving NDR (Non-Delivery Reports) for mail failures shall forward the same to ICT Support or ICT Systems Administrators for trouble shooting. Staff are however required to ascertain, before launching a complaint that the address of the recipient is correct and free from typos.

Complaints about mail receipt failure should always be accompanied by the sender address and the recipient address. This will enable the administrators to narrow down to the particular case and give a report and advice to the affected user the soonest possible (within 30 minutes or as per the SLA).

6.0. Internet Policy

Only users authorized through their line managers are allowed to browse during work time. Other users can browse after working

hours and during weekends. Users shall not assume any privacy while browsing the internet. Browsing is always monitored and some sites are restricted by use of internet monitoring software. Any user who is blocked from accessing a site which facilitates his work can, through his/her line manager, get in touch with systems administrators to open up the site as long as the site is safe to access and does not compromise KenGen network. Pornographic sites are always blocked.

7.0 Network Security And Access Policy

Firewalls and Intrusion Detection systems shall be used across the entire KenGen network to monitor and prevent hackers, viruses and worms including all other forms of attack. The in-charge of network shall ensure that this policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances and top management approval.

All computers hooked into the network shall mandatorily have an up-to-date antivirus software to prevent viruses and all other forms of malicious code. Additionally the computers must have all unnecessary services eg. WWW disabled to prevent intrusion. It shall be the responsibility of ICT support to ensure that this policy is adhered to failure to which disciplinary action shall be executed as per management approval. All staff are also expected to seek authority from ICT support before hooking any laptop to the network. Staff are also expected to timely report outdated versions of antivirus for action to ICT support. Failure to do so may result to disciplinary action.

All servers shall likewise have antivirus and a form of monitoring to ensure that only authorised users have access. The senior systems administrator and/or his appointee shall enforce this policy failure to which disciplinary action may be executed against him/her depending on circumstances and top management's approval.

8.0 Data Centre and DRC Access Policy

Only authorised ICT personnel are allowed to access the ICT data center and DRC. All other persons must be accompanied by authorised staff and must sign a visitor's book. Responsibility: Senior Systems Administrator and his/her appointee. Consequence: Disciplinary action on the staff violating this policy.

9.0. Policy on Printers, Telephone lines, fax and Copiers.

Staff are expected to use the above responsibly. Irresponsible/excessive use of the above for personal purposes is discouraged, and may, depending on the line manager's determination and management's approval lead to disciplinary action which may include, but not limited to, denial of the service.

10.0. Policy on Passwords

10.1 Do not disclose to anyone (See Note 2 below)

10.2 Do NOT write it down.

10.3 Should be a combination of alphanumeric and special characters(!_?\$^*#), i.e complex, but easy to remember.

10.4 Passwords must be at least six (6) characters.

10.5 Users are required to change their passwords at least every three months.

10.6 Passwords shall lock for every three unsuccessful attempts.

10.7 The maximum number of sessions per user shall be three(3).

10.8 Password Management

10.8.1 This shall be the responsibility of Senior Systems Administrator(SSA) and/or his appointee(s).

10.8.2 A user whose password has expired, or account locked shall (upon request through IT support) be assigned an initial password by the systems administrator. The affected user must change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.

11.0. Policy on ICT Related Training

11.1 Every section within ICT department shall identify training needs every beginning of financial year and forward to the ICT divisional committee.

11.2 The ICT divisional committee shall analyse the trainings relevant for every section to make sure that the training requirements are relevant to the various sections staff and within

budget and forward the names and requirements to the manager in charge of ICT.

11.3 The manager in charge of ICT shall, upon his approval, forward the training requirements to Human Resource and Administration for implementation.

12.0. Policy on Online Subscriptions

12.1 Section heads shall have the mandate to do online subscriptions on behalf of their sections, but in consultation with the manager in charge of ICT department. For security reasons, the section heads shall use their own money or cards to subscribe and only receive re-imburements upon presentation of prove of payment.

12.2 Section heads are advised to be careful when making online payments/subscriptions as KenGen shall NOT be liable for any losses incurred through online/internet transactions.

13.0 Policy on ICT Disaster Recovery

ICT Disaster recovery shall be carried out as outlined in the ICT Services Disaster Recovery Plan.

14.0 Policy on ICT Technical Assistance Request & Complaints.

All ICT technical assistance requests shall be channelled through the centralised helpdesk system. Requests and/or complaints made

through other means e.g. telephone shall be given less priority than requests made through the helpdesk system.

Responsibility: All staff.

15.0. Miscellaneous

15.1 Hardware and Software: All purchases should be approved by the ICT Manager, preferably through the IT budget.

15.2 Installing Software: Get permission from IT Support or ICT Administrators before you install any software (including public domain software - see Note 6) on equipment owned and/or operated by KenGen.

15.3 Data transfer and storage on the network:

15.3.1 Keep master copies of important data on your profile eg. My Documents folder. Otherwise it will not be backed up and is therefore at risk. This applies to managers. If you change your computer, you should inform IT support to update the DLO agent which facilitates backup of your profile. Personal files should be kept to minimum.

15.3.2 Ask for advice from IT Support and/or IT Administrators if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill. (See Appendix I: Best Practices on transmitting attachments & pictures)

15.3.3 Be considerate about storing personal (non- KenGen) files on KenGen's network. (Note 7).

15.3.4 Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disc space unnecessarily.

15.4 Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, playing computer games and browsing the Internet) is permitted so long as such use does not:

- incur specific expenditure for KenGen
- impact on your performance of your job (this is a matter between each member of staff and their line manager)
- break the law
- bring KenGen into disrepute.

15.5 Care of equipment:

- Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.
- Don't take food or drink into rooms which contain specialist equipment like servers (Note 8). Access to such rooms are limited to systems administrators and other authorised staff.

16.0. Revision

This policy shall be revised on a quarterly basis. Changes necessitating revision shall include changes in technology, statutory

regulations and any other reasons as may be determined from time to time by the manager in charge of ICT.

NOTES

- (1) In-house software: This is software written by staff or volunteers using KenGen's equipment. It is KenGen's property and must not be used for any external purpose. Software developers employed at KenGen are permitted to take a small "portfolio" of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the IT Manager.
- (2) Personal passwords: Disclosure to other staff, volunteers or external agents: This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the IT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting IT Support) as soon as the task is completed. Users shall be prompted to change their passwords from time to time to enhance system security.
- (3) Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people. Systems administrators can tell you what these are and how to use them.
- (4) Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, eg home or cybercafe. IT Support can advise you on setting up such an account.
- (5) Subject box prefixes: These are "U:" for Urgent', 'FYI' for your information and 'AC:' requires action, 'FYI:' For Your

Information, 'FYA:' For Your Action. If the email is a very brief message confined solely to the subject line, it should in addition be prefixed with '**' to indicate "just read this line".

- (6) Public domain software or Freeware: This is software that is available free of charge, usually by downloading from the internet.
- (7) Personal Data: As a guideline, keep your personal data to minimal say 1GB. Ten emails require 0.15MB on average (depends a lot on whether they have attachments). A 10-page word processed document requires about 0.1MB. Screen saver images require much more disc space and vary greatly - some may be as large as 2MB.
- (8) Computer Room/Data Center: This is the room on the first floor of KenGen Stima Plaza building which contains servers and communication equipment. The door should be closed at all times and entry restricted to authorized persons only.

APPROVAL

This ICT Policy document in its initial form has received the following review and approvals from KenGen management:

Prepared By:

KenGen ICT Policy Team

Signature & Date:

Checked By:

ICT Manager

Signature & Date:

Authorized By:

Director, Finance & Commercial

Signature & Date:

ABBREVIATIONS

KenGen – Kenya Electricity generating Company Ltd.

DRC – Disaster Recovery Center/Site

ICT – Information Communication Technology

IT – Information Technology

FYI – For Your Information

NDR – Non Delivery Report

FYA - For Your Action

SLA – Service Level Agreement

ISO – International Organisation of Standards

APPENDICES

APPENDIX I

(Sourced from MS Office 2007 Online help)

Best practices to use when sending pictures and attachments: (Source: Microsoft Office 2007 Online Help)

- **Post or publish large attachments** If you're sending attachments or pictures to someone within your organization, use a file share on your computer or a shared network resource. You can include a link to that location in your e-mail message. Or, if your organization uses Microsoft Windows SharePoint Services 3.0, post the attachments in a document workspace or in a [SharePoint library](#) and point users there. Either way, everyone uses only one copy of the files.
- **Limit your attachments to under 2 megabytes (MB)** This is a general guideline; for slower, dial-up connections you should use a much smaller size, such as 250 kilobytes (KB). If you must send larger attachments, verify the maximum size of the message that you can send. Your mail server administrator or ISP can tell you this. Likewise, ask the recipient what their maximum limit is. Finally, consider the recipient's Internet connection speed. Downloading a large attachment on a dial-up Internet connection can take a long time.
- **Send multiple attachments by using several e-mail messages** Multiple smaller messages have a higher likelihood of being delivered versus one large message. This technique might help you avoid per-message limits, but the recipient's mailbox limit can still be exceeded. Any messages received after a person's mailbox has reached its storage limit are typically rejected.
- **Use compressed graphic file formats** There are far too many graphic file formats to list here, but of the most commonly used, the best picture file formats for e-mail are .jpg, .png, and .gif. The largest graphics file formats are those that are not saved in a compressed file format, such as .tif and .bmp (the default file format of Windows Paint).
- **Use smaller original files** The size of a photo taken by a digital camera is typically large, even when saved in a compressed file format such as .jpg. It's not uncommon for a single picture to be several megabytes. Remember that the size of the e-mail message will increase by approximately one-third while in transit on the Internet. Use a lower resolution setting on your camera when taking a digital photo. Use compressed file formats such as .jpg. In a graphics program, crop photographs to the essential content. Use the [automatic picture reduction feature](#) in Windows and Microsoft Office Outlook.

- **Use smaller original files** The size of a photo taken by a digital camera is typically large, even when saved in a compressed file format such as .jpg. It's not uncommon for a single picture to be several megabytes. Remember that the size of the e-mail message will increase by approximately one-third while in transit on the Internet. Use a lower resolution setting on your camera when taking a digital photo. Use compressed file formats such as .jpg. In a graphics program, crop photographs to the essential content. Use the [automatic picture reduction feature](#) in Windows and Microsoft Office Outlook.
- **Use a file compression utility** In addition to third-party utilities, Windows XP and Windows Vista include a [file compression utility](#) that uses the compressed .zip file format. Many attachment file formats can be reduced with the use of a compression utility. The amount of reduction will be minimal with some file formats that are already saved in a compressed format. For example, a Notepad .txt text file will reduce dramatically, while a .jpg image will not. The .jpg file format is already a compressed file format. You can find more information about using file compression in Windows Help.
- **Review your Sent Items folder** By default, a copy of each message that you send is kept in the Sent Items folder. This increases the size of your Outlook data file, which can, with certain accounts, count against your mailbox size limit because the sent items are saved on your mail server.