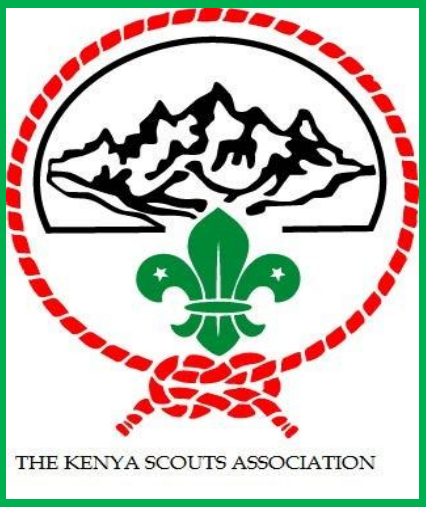

THE KENYA SCOUTS ASSOCIATION

INFORMATION TECHNOLOGY POLICY FRAMEWORK

MARCH 2016

KENYA SCOUTS ASSOCIATION, ROWALLAN SCOUT CAMP, JAMHURI PARK, KIBERA DRIVE+254 020 202 0819, + 254 733 919 333, P.O BOX 41422-00100, NAIROBI KENYA
www.kenyascouts.org, info@kenyascouts.org

Contents

ACRONYMS/ABBREVIATIONS

AIDS	Acquired Immunodeficiency Syndrome
DANIDA	Danish International Development Agency
DES	Data Encryption Standard
FTP	File Transfer Protocol
HIV	Human Immunodeficiency Virus
ICT	Information & Communication Technology
IT	Information Technology
KSA	Kenya Scouts Association
NGO	Non- Governmental Organization
PC	Personal Computer
PDA	Personal Data Assistant
PGP	Pretty Good Privacy
UN	United Nations
UNDCP	United Nations International Drug Control Programme
WAP	Wireless Application Protocol
WOSM	World Organization of Scouting Movement

1.0 Background of KSA

THE KENYA SCOUTS ASSOCIATION EDUCATIONAL PROPOSAL

Kenya Scouts Association (KSA) is a registered member of the World Organization of the Scouts Movement (WOSM). It is a voluntary, non-political and educational Movement for young people open to all without distinction of origin, race, gender, creed or ethnic/tribal background in accordance with the purpose, principles and method as conceived by the founders as stated below;

a) Purpose

To contribute to the development of young people in achieving their full physical, intellectual, emotional, spiritual, social, and character potentials as individuals, as responsible citizens and as members of their local, national, regional and international communities.

b) Principles

- Duty to God

Adherence to spiritual principles. Loyalty to the religion that expresses them and acceptance of duties resulting there from.

- Duty to others

Loyalty to our country in harmony with the promotion of local, national, regional and international peace, understanding and co-operation/integration.
Participation in the development of society with recognition and respect for the dignity of ones fellow man and for the integrity of nature.

- Duty to self

Responsibility of the one's self; realization of ones right to develop, learn and grow, learning to assert oneself, make ones decision, set aims and identify the necessary steps to achieve ones full potentiality.

c) Method

It is a system of progressive self-education that should be applied to all sections, taking into account the socio-cultural environment of the young people.
The Scout method is applied in the following ways:

i. Law and promise.
ii. Learning by doing.
iii. Membership of small groups (patrol system) requiring adult guidance, progressive discovery and acceptance of responsibility and training towards self-governance directed towards the development of competence, self-reliance, honesty and leadership skill objectives.
iv. Progressive and stimulating programs (progressive scheme) consisting of varied activities based on one's own interest including games, useful skills and service to community, all taking place largely in an outdoor setting.
v. Symbolic framework or symbolic background where the scouts relate to their socio-cultural background in order to have a programmed that has a national touch.
vi. Relationship between adults and young people where leaders have the responsibility to keep an eye on the young ones especially the Sungura, as they are delicate majority.
vii. Life in nature, it is not just animals, trees, rivers etc. for scouts. Nature is a club where one can enjoy themselves, a laboratory where one feels closer to God and can worship Him in one's own way.

KSA Vision
Creating a better world.

KSA Mission
Educating young people to play a constructive role in the society.
This is achieved by:-

i. Involving the youth throughout their formative years in a non-formal educational process.
ii. Using a specific method that makes each individual the principle agent in ones development as a self-reliant, supportive, responsible and committed person.
iii. Assisting them to establish value system based upon spiritual, social, and personal principles as expressed in the scouts law and promise.

Situation in Kenya
Kenya like many other countries in Africa is faced with unique challenges requiring unique interventions/responses. This makes us give Scouting a specific orientation with the aim to responding to the needs and aspirations of the Kenyan youth thus making Scouting a reliable actor in the Kenyan civil society.

The Kenyan society is still facing a number of challenges notably unemployment, violation of human rights, oppression, poverty, ethnic, strives, high school dropout rates, poor infrastructure, breakdown in family values and morals and gender disparity/imbalance, etc.
Secondly, our natural resources are over exploited without replacement leading to desertification, droughts and floods. Everywhere in the country, the youth are threatened

by pandemic diseases i.e. HIV/AIDS, drugs abuse and many of them have found themselves in difficult circumstances especially on streets without basic needs i.e. food, shelter, clothing and lack of education. Under development of rural areas has also accelerated rural-urban influx leading to uncontrolled urbanization and the development of slums and shanties.

As an Association, we have quite a number of opportunities and strengths that can be harnessed to reverse this situation namely;

i. Large membership of young boys and girls in the Association.
ii. Goodwill from the members of the public and the government.
iii. Good organizational structure of co-ordination and networking throughout the country.
iv. Large number of qualified trainers and scout leaders.
v. Availability of resource and reference materials.
vi. Willing partners e.g. Africa Regional office/WOSM, Donor and UN agencies i.e. UNIFA, DANIDA, UNDCP, and other NGOs, Government departments and ministries.
vii. Existence of a rich youth programme that is able to address the contemporary issues facing out youth.

Today, KSA in co-operation with various partners is involved in a number of community development programmes giving young people opportunities to improve the quality of life in their community and acquire the necessary skill and attitude to enable them become real agents of development. These include children in difficult circumstances project, peace and reconciliation campaigns, reproductive health and HIV/AIDS education, drug abuse control, environmental awareness, human rights advocacy, etc.

The contribution scouting can give to the development of this county in the long term is to train the future leaders that Kenya needs to overcome its problems. This is the main reason why we are making this education proposal and commitment for the Kenyan youth.

Our Commitment

We, the Kenya Scout Association want to contribute in preparing free, supportive, responsible and committed citizens, who are needed to build a better future for Kenya.

They will be;-

i. Men and women of character Integrity responsible and self-reliant, constant and true to the word, able to value human labor and to build their family on love; aware of their won dignity and that of others, able to share with everybody joyfully and affectionately.
ii. Agent of development ready to serve other, involved in their community, defenders and respecters of other people's rights, pledged to democracy and committed to development, lovers of justice and promoters of peace.
iii. Creative persons keen to leave the world better than they found it, able to strive for the integrity of the natural world, learning continually and searching for ways to solve problems and do their work well.

iv. Spiritual people free from the hunger to possess, with a transcendental sense of life, able to open their hearts to God, live their faith joyfully and make it part of their daily life, open to dialogue and understanding and able to respect others' cultural traditions and religious beliefs.

v. Therefore out choice is to act as educators, as supporters of out youths to work with all the citizens who believe in young people as real agents of a brilliant future for all Kenyans and the world at large.

KSA Information Technology Policy

1.2 Introduction

This IT Policy also is put in place for the protection and guidance of the organization and individuals by giving users ground rules for acceptable use of IT equipment. This policy is divided into various components for effective management of IT.

1.3 Definition of Terms

- Server - A Server is defined as an internal Kenya Scouts Association Server.
- Delivered Direct – A Signature is required to prove delivery
- Approved Electronic File Transmission Methods - Includes supported FTP clients and Web browsers.
- Envelopes Stamped Confidential - stamp the word confidential on the envelope before delivery/postage.
- Approved Electronic Mail - Includes all mail systems supported by the IT Support Team (official emails using the Associations email platforms)
- Approved Encrypted email and files - Techniques include the use of Data Encryption Standard (DES) and Pretty Good Privacy (PGP).
- Company Information System Resources - include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
- Expunge - To reliably erase data on a PC
- Individual Access Controls - Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. Use passwords
- Physical Security - Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.
- User Authentication - A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

2.0 SERVER SECURITY

2.1 Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about preventing these acts.

2.2 Scope

All employees, contractors, consultants, temporary and other workers at Association must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by or registered under the Kenya Scouts owned internal network domain.
This policy specifies requirements for equipment on the internal KSA network.

2.3 General Requirements for Server Security

i. All internal servers deployed at the Kenya Scouts Association shall be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Each operational group shall establish a process for changing the configuration guides, which includes review and approval by the Association.
ii. Servers shall be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    i. Server contact(s) and location, and a backup contact
    ii. Hardware and Operating System/Version
    iii. Main functions and applications, if applicable
    iv. Information in the corporate enterprise management system must be kept up-to-date.
    v. Configuration changes for production servers must follow the appropriate change management procedures.
iii. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

2.4 Configuration Requirements

i. Operating System configuration shall be in accordance with KSA approved guidelines as indicated in this document's appendices.
ii. Services and applications that will not be used must be disabled where practical.

iii. Access to services shall be logged and/or protected through access-control methods such as a web application firewall, if possible.
iv. The most recent security patches shall be installed on the system as soon as practical, the only exception being when immediate application would interfere with Associations business requirements.
v. Trust relationships between systems are a security risk, and their use shall be avoided. Do not use a trust relationship when some other method of communication is sufficient.
vi. Always use standard security principles of the least required access to perform a function.
vii. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access shall be performed over secure channels, (for example using encrypted network connections).
viii. Servers shall be physically located in an access-controlled environment and are specifically prohibited from operating from uncontrolled areas.

2.5 Monitoring

All security-related events on critical or sensitive systems shall be logged and saved as follows:

i. All security related logs shall be kept online for a minimum of 1 week.
ii. Daily incremental tape backups shall be retained for at least 1 month.
iii. Weekly full tape backups of logs shall be retained for at least 1 month.
iv. Monthly full backups will be retained for a minimum of 2 years.

2.6. Reporting

Security-related events shall be reported to the KSA IT department, who will report these incidents to relevant the National Executive Commissioner. Security-related events include, but are not limited to:

i. Port-scan attacks
ii. Evidence of unauthorized access to privileged accounts
iii. Irregular occurrences that are not related to specific applications on the host.

2.7 Policy Compliance

The Kenya Scouts Association staff, volunteers, consultants shall be expected to comply with this policy by signing a compliance agreement. The relevant committee shall be responsible for the compliance of this policy.

2.8 Non-Compliance

Violated this policy shall be subject to disciplinary action.

3.0 IT AUDIT

3.1 Scope

This policy covers all computer and IT devices owned or operated by the Kenya Scouts Association. This policy also covers any computer and IT device that are present on the Associations premises, but which may not be owned or operated by Association.

3.2 Policy

When requested, and for the purpose of performing an audit, any access needed shall be provided to members of the Kenya Scouts Association IT Audit team.
This access may include:

i. User level and/or system level access to any computing or IT device
ii. Access to information (electronic & hardcopy) that may be produced, transmitted or stored on the Associations premises
iii. Access to work areas
iv. Access to log traffic on the Associations networks.

3.3 Enforcement

The relevant committee shall be responsible for the enforcement and compliance of this policy.

4.0 INFORMATION SENSITIVITY / PROTECTION

The Information Sensitivity IT guidelines is intended to help employees, volunteers and consultants to determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Kenya Scouts Association without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

4.1 Information classification

All Kenya Scouts Association information is categorized into two main classifications:

i. KSA Public information
   KSA Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the Association.

ii. KSA Confidential information

- KSA Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as financial statements and other information integral to the success of the Association. Also included in KSA Confidential is information that is less critical, such as personnel information which does not require as stringent a degree of protection.
- A subset of KSA Confidential information is the Associations "Third Party Confidential "information. This is confidential information belonging or pertaining to another corporation which has been entrusted to the Kenya Scouts Association by that company under non-disclosure agreements and other contracts.

The Kenya Scouts Association personnel are encouraged to use common sense judgment in securing KSA Confidential information to the proper extent. If an employee, volunteers and consultants is uncertain of the sensitivity of a particular piece of information, he/she should contact the Head of Department or Executive Commissioner for guidance.

4.2 Sensitivity guidelines

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels.

4.2.1 Minimal Sensitivity

This includes general corporate information; some personnel and technical information.

- The words 'KSA Confidential" shall be written or designated in a conspicuous place on or in the information in question.
- If no marking is present, the Associations information is presumed to be "KSA Confidential" unless expressly determined to be the Associations Public information by an employee at the Association with authority to do so.
- Access to this type of information is limited to KSA employees, consultants, volunteers among others.
- Distribution of this type of information within the Association is through Standard interoffice mail, approved electronic mail and electronic file transmission methods.
- Distribution of this type of information outside of the Association shall be through internal mail, public or private carriers, approved electronic mail and electronic file transmission methods.
- Electronic distribution of this information shall be sent to only approved recipients.
- This information shall be keep from view of unauthorized people by erasing whiteboards and not leaving in view on tabletops. Machines shall be administered with security in mind.
- For protection from loss, electronic information should have individual access controls where possible and appropriate.
- This type of information shall be disposed/destroyed by shredding or burning of outdated paper information. Electronic data shall be expunged/cleared. Information

media shall be reliably erase or physically destroy. For key information proper authorization shall be obtained before disposal.

- The penalty for deliberate or inadvertent disclosure of this information is up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.2.2 More sensitive

This includes business, financial, technical, and most personnel information

- As the sensitivity level of the information increases, the information shall be labeled as "KSA Internal Use Only".
- This information will be accessed by KSA employees, volunteers and consultants and non-employees with signed non-disclosure agreements who have a need to know basis.
- Distribution of this type of information within the Association is through Standard interoffice mail, approved electronic mail and electronic file transmission methods.
- Distribution of this type of information outside of the Association shall be through mail or approved private carriers.
- Electronic distribution of this information shall be sent to only approved recipients within the Association but should be encrypted or sent via a private link to approved recipients outside of Associations premises.
- Individual access controls are recommended for electronic information storage.
- This type of information shall be disposed/destroyed by shredding or burning of outdated paper information. Electronic data shall be expunged/cleared. Information media shall be reliably erase or physically destroy. For key information proper authorization shall be obtained before disposal.
- The penalty for deliberate or inadvertent disclosure of this information is up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.2.3 Most Sensitive:

This information includes operational, personnel, financial & technical information integral to the success of the Association.

- To indicate sensitivity, this information shall be labeled as follows: "KSA Internal", "KSA Restricted", or "KSA Confidential".
- Users to be informed that this information is very sensitive and should be protected as such.
- Only those individuals (KSA employees, consultants, volunteers and non-employees) designated with approved access and signed non-disclosure agreements will have access to this information.
- Distribution of this information within KSA shall be in the form of direct delivery where a signature is required or by envelopes stamped KSA confidential/restricted/KSA internal or approved electronic file transmission methods.

- Distribution of this information outside of KSA shall be through internal mail, direct delivery; signature required and approved private carriers.
- Electronic distribution of this information shall be sent to only approved recipients within the Association, but it is highly recommended that all information be strongly encrypted.
- Individual access controls are very highly recommended for electronic information storage.
- Information shall be stored in a physically secured computer.
- This type of information shall be disposed/destroyed by shredding or burning of outdated paper information within KSA. Electronic data shall be expunged/cleared. Information media shall be reliably erase or physically destroy. For key information proper authorization shall be obtained before disposal.
- The penalty for deliberate or inadvertent disclosure of this information is up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.3 Enforcement

The relevant committee shall be responsible for the enforcement and compliance of this policy.

5.0 WIRELESS COMMUNICATION

The procedures on wireless communication prohibits access to the Kenya Scouts networks via unsecured wireless communication mechanisms.

5.1 Wireless Communication Data Devices

This covers data communication through devices such as personal computers, cellular phones, PDAs, among others connected to any of the Kenya Scouts Associations internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the Associations networks do not fall under the purview of this policy.

To comply with this wireless data communication requirements, the IT department shall

- Maintain a hardware address that can be registered and tracked.
- Support strong user authentication which checks against an external unauthorized usage.
- Only authorized persons are allowed to use the wireless services at the Kenya Scouts Association
- Wireless services to be safe guarded via use of a password which shall be changed on a monthly basis.

5.0 Enforcement

The relevant committee shall be responsible for the enforcement and compliance of this policy.

6.0 REMOTE ACCESS

6.1 Standards for connecting to KSA network remotely

These standards are designed to minimize the potential exposure to the Kenya Scouts Association from damages which may result from unauthorized use of Associations resources. Damages include but are not limited to the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Association's internal systems.

Remote access implementations that are covered by this policy include, but are not limited to, use of dial in modems, cable modems, internet, mobile phones, cloud based access, dual homming, personal digital assistant (PDA) Wireless Application Protocol (WAP) and Personal computers.

It is the responsibility of the Kenya Scouts Association employees, consultants, vendors and agents with remote access privileges to the Kenya Scouts Association corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Association.

General access to the Internet for recreational use by immediate household members through the KSA Network on personal computers is not permitted. This also includes access to inappropriate content and prohibited sites

6.2 Requirements

i. Secure remote access shall be strictly controlled. Control shall be enforced via password authentication.
ii. At no time shall any employee, volunteer, consultant provide their login or email password to anyone, not even family members.
iii. Employees with remote access privileges shall ensure that their KSA owned or personal computer or workstation, which is remotely connected to the Association's corporate network, is not connected to any other network at the same time.
iv. Employees, volunteers, consultants with remote access privileges to the KSA corporate network must not use non - KSA accounts or other external resources to conduct the KSA business, thereby ensuring that official business is never confused with personal business.
v. All hosts that are connected to the KSA internal networks via remote access technologies must use the most up-to-date anti-virus software.

6.3 Enforcement

The relevant committee shall be responsible for the enforcement and compliance of this policy.

7.0 ANTI - VIRUS GUIDELINES

i. All computers and Association lap tops shall be installed with an updated corporate antivirus software.
ii. Users of the Association's laptops and computers shall run the corporate standard, supported anti-virus software updates.
iii. Employees and consultants shall download and install anti-virus software updates as they become available.
iv. Any files attached to an email from an unknown, suspicious or untrustworthy source shall not be opened. These attachments shall be deleted immediately, then double deleted by emptying the trash. If in doubt consult with the IT department.
v. Employees and consultants shall delete spam, chain, and other junk email without forwarding the same.
vi. Disk sharing with read/write access shall be avoided.
vii. Disks from an unknown source shall not be used.
viii. Back-up of critical data and system configurations and storage of the data in a safe place shall be done on a daily and monthly basis.
ix. When the anti-virus software is disabled, employees and consultants shall not run any applications that could transfer a virus, for example email or file sharing.
x. The IT team shall periodically check the machines to ensure system configurations and anti-virus is up to date.
xi. Virus and malware scanners shall be kept up to date.

8.0 IT MAINTENANCE

IT maintenance (hardware and software) shall be done regularly to ensure IT system work without fault. This includes regularly checking and updating IT systems.

i. All IT software licenses shall be up-to-date.
ii. Anti-virus programme shall be efficient and up to date.
iii. IT system passwords shall be changed twice a year.
iv. An IT maintenance daily, weekly, monthly schedule shall be put in place and followed strictly.
v. Users are encouraged to back up daily on external hard drives and on the server.
vi. Automation of backups and software updates shall be done.
vii. IT systems documentation shall be updated. This includes all software licenses plus renewal dates and the age of any hardware such as screens and keyboards. This will aid in upgrading or replacing of these systems.
viii. Monitoring of IT systems shall be made part of IT maintenance
ix. IT online security shall be checked and maintained on a monthly basis.

x. Outsourcing of IT maintenance to be considered whenever possible

9.0 POLICY IMPLEMENTATION AND AMENDMENT

1. The Information Technology Committee shall be charged with responsibility of the administration and management of the ICT Policy Framework
2. In order to remain faithful to the principles on which it is based, the Kenya Scouts Association, Information Policy Framework shall be reviewed regularly by the ICT Committee.
3. Final approval shall be sought from the National Executive Committee for any amendments made on this policy.
4. The National Executive Committee shall be kept updated on the progress of the implementation of this policy.
5. This Policy Framework is subject to The Kenya Scouts Association Constitution of 2012.
6. As need arises, this policy can be amended subject to approval of such a move by the National Executive Committee after receiving the suggestions and justification of such a move from the ICT committee.
7. The IT Policy Framework of Kenya Scouts Association as legal document may be cease to exist in the event that it is repealed by the National Executive Committee or there is a reorganization or merger of subcommittees by the National Executive Committee.

10. 0 RELATED STANDARDS, POLICIES AND PROCESSES

i. The KSA Communications Policy
ii. The KSA Brand Policy