

UGANDA RED CROSS SOCIETY

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY GUIDELINE



Version: ii

Updated: 2008

TABLE OF CONTENTS

1.1 INTRODUCTION.....	1
1.2 SCOPE OF THE POLICY.....	2
1.3 RELEVANCE OF THE POLICY.....	2
1.3.1 INFORMATION AND COMMUNICATION TECHNOLOGY TODAY	2
1.3.2 RAPID CHANGING TECHNOLOGY.....	3
1.3.3 ICT EXPERTISE SCARCITY	3
1.3.4 SCARCITY OF OTHER RESOURCES	4
1.3.5 STRATEGIC RELEVANCE	4
1.3.6 CHANGING WORKING HABITS AND PROCESSES.....	4
1.4 COORDINATION OF ICT POLICY.....	5
2.0 ICT POLICIES AND GUIDELINES.....	6
2.1 INTERNET USER POLICY	6
2.1.1 <i>Personal Use of the Internet/Online Services.....</i>	6
2.1.2 <i>Downloading from the Internet/Online Services</i>	7
2.1.3 <i>Pornography.....</i>	7
2.2 EMAIL USAGE POLICY GUIDELINE	8
2.2.1 <i>The main purpose of Email Services.....</i>	8
2.2.2 <i>Email Services Abuse.....</i>	9
2.2.3 <i>Personal use of URCS Emails.....</i>	9
2.3 OFFICE COMPUTING SERVICES POLICY GUIDELINE.....	11
2.3.1 <i>Recommendable Office Applications and Operating Systems.....</i>	11
2.4 ICT SECURITY POLICY GUIDELINE	12
2.4.1 <i>Reasons for URCS ICT Security.....</i>	13
2.5 PHYSICAL SECURITY.....	14
2.6 NETWORK SECURITY.....	15
2.6.1 <i>Network General policy Guidelines.....</i>	15
2.6.2 <i>Restricted Software and Hardware.....</i>	17
2.6.3 <i>Wasting Network Resources</i>	17
2.6.4 <i>Online Game Playing.....</i>	18
2.6.5 <i>Use of Mobile Computers (laptops).....</i>	18
2.6.6 <i>Privacy of expectations.....</i>	19
2.6.7 <i>Password Management.....</i>	19
2.7 HARDWARE MANAGEMENT POLICY GUIDELINE	22
2.7.1 <i>Hardware Security User Guideline</i>	22
2.7.2 <i>Hardware Personal use</i>	24
2.8 URCS SOFTWARE MANAGEMENT AND USAGE GUIDELINES.....	25
2.8.1 <i>Software License Management</i>	25
2.8.2 <i>Software Acquisition</i>	25
2.8.3 <i>Software Installation.....</i>	26
2.8.4 <i>Using Company Software on Home Computers</i>	27
2.8.5 <i>Software Audits.....</i>	27
2.8.7 <i>Discipline.....</i>	28

3.0 IDENTIFIED ICT SERVICES AND INFORMATION SYSTEMS.....	29
4.0 END USER SKILLS DEVELOPMENT.....	31
4.1 HUMAN CAPACITY DEVELOPMENT	31
5.0 POLICY IMPLEMENTATION.....	33
5.1 ROLE OF SENIOR MANAGEMENT	33
5.2 USER RESPONSIBILITIES	33
5.3 IMPLEMENTATION TEAM.....	34

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY FOR UGANDA RED CROSS SOCIETY EMPLOYEES AND VOLUNTEERS

1.1 Introduction

This Policy is an update of the previous policy, care has been taken to eliminate irrelevant articles that were found inapplicable currently to the management of ICT resources for Uganda Red Cross Society due to the rapid change in technology. Also the policy language has been revised to enable non-technical users of the policy to easily understand and interpret.

The Uganda Red Cross Society's mission is to mobilize the power of humanity for improving the lives of the vulnerable, while adhering to the seven principles of the Red Cross/Red Crescent Movement. Increasingly, the society is called upon to deliver more and better services to a growing population. Much of this productivity increase has come about through the use of modern information technology.

The relationship between URCS, its employees and volunteers who implement the functions of the society is based on trust. Consequently, employees and volunteers are expected to follow rules and regulations and to be responsible for their own personal and professional conduct while using ICT resources of the National Society.

1.2 Scope of the Policy

This policy applies to all staff of the Uganda Red Cross Society irrespective of the level of position and responsibilities attached and volunteers who are the users of the National Society's ICT resources. It spans all areas of operation starting from the National headquarters, all regions and branches where ICT is applied to facilitate implementation of URCS activities.

1.3 Relevance of the Policy

1.3.1 Information and Communication technology today

Any modern organization today is critically dependent on the smooth functioning of Information and Communication Technology (ICT) and its ICT services. Smooth functioning and running can be assured only if establishment, operation and extension of ICT and ICT enabled functions is effected within a clear policy framework that takes full recognition of the organization's overall strategic goals. Uganda Red Cross Society recognizes this critical need and therefore agreed to review its ICT policy, as detailed in this document, comprising the general role and nature of ICT in its functions. It draws:

- The anticipated services that are considered of strategic relevance to the Uganda Red Cross Society.
- The principles of Uganda Red Cross Society local area network (LAN) infrastructure and
- The major characteristics of ICT management environment to assure sustainable, efficient, user-friendly, robust and secure operations and deployment of all anticipated ICT services.

The ICT policy reflected in this document is a result of the Society's wide needs assessment, careful studies and decision making by the management. The ICT policy by virtue of its approval by the URCS management can be highly considered to be the primary guideline for structured ICT implementation planning and decision making in the URCS strategic plan.

Like other URCS resources such as staff, assets, ICT services and systems require good planning, controlling, investing and maintenance. The development of a general policy for assimilating ICT and ICT services into the Society's operations has grown steadily and more important. To be effective, the policy planning process must deal simultaneously with the realities of the Society's general planning culture, existing technologies and systems and the relevance of ICT to the Society's general long-term goals.

1.3.2 Rapid changing technology

As technology changes, planning become increasingly important in order to avoid incompatibility and inaccessibility, therefore, there is need to have standards, procedures and guidelines that are revisited on time and hence the need for the ICT policy for URCS.

1.3.3 ICT expertise scarcity

The scarcity of highly trained and advanced experienced ICT specialist, software developers, systems/Network administrators, coupled with the changing technology, requires that organizations invest in training their ICT support staff, end users and volunteers over time on order to catch up with the speed of ICT dynamics. This can be implement if it is part of the Policy issues that can easily be recognized by the management.

13.4 Scarcity of other resources

The limited availability of financial and managerial resources is yet another factor to consider for high level ICT planning. ICT should be one of the many strategic investment opportunities for URCS in order to improve its records management, inventory and Management Information System (MIS). This also needs to be documented as some of the key standards and guidelines for the ICT users and management.

1.3.5 Strategic relevance

ICT may be more significant to some functions within the Society than others. This notion of differing strategic relevance is critical to the understanding the wide diversity of potential practices that can be used to integrate ICT within the organization.

Successful development, implementation and deployment of ICT services depends on careful and realistic planning, although planning as such cannot guarantee success. The risks inherent to today's ICT environment, with changing technology and increasing user demands, require that IT specialists appraise ICT and application trends, so that strategic decisions on change can be taken without adverse impact on the Society's operations.

1.3.6 Changing Working habits and Processes

The process of integration of ICT services into the organization must be properly managed. If it is poorly managed ICT will not evolve into a well-functioning and accepted system but, instead, into a collection of disjointed islands of technology, that finally can only be managed with great difficulty. Implementation of ICT is not simply an introduction of new technology, but a complete re-thinking of how the organisation's functions are achieved.

Success only comes when people are able and willing to change their working habits and thinking processes. Without this change of thinking and doing when new technology or new ICT services are implemented, technical success is likely to be accompanied by the organizational failure.

1.4 Coordination of ICT policy

Top management must play a significant role in ensuring that these policies are developed and that they evolve over time. On the other hand both ICT professionals and users must understand the implications of their roles and possible conflicts.

2.0 ICT Policies and Guidelines

2.1 Internet user Policy

2.1.1 Personal Use of the Internet/Online Services

Introduction: The Internet has become one of the most valuable communication services for most organizations. It provides access to a wealth of information sources located on the computer systems around the world. In the URCS, access to the Internet includes the following components:

- a) Web Browser application running on every workstation to search, download and display visual information sources.
- b) Appropriate internal network infrastructure and equipment linking internal network to the Internet Highway.

Intranet Services may be used for on-line publication of part of the organization's vital documents such as the constitution, standing regulations, The Weekly eye, The Humanitarian etc. At times providing Intranet services requires dedicated software and a dedicated computer reserved for it (server).

Policy Statement: All staff and volunteers of URCS must use the Internet/online services without interfering others sharing the same service on the Uganda Red Cross Internet and Email servers.

Use of continuous data streams technology on the Internet and other like forms of technology would also degrade the performance of the entire network and can be inappropriate use.

Policy Penalty: Any personal use that could cause congestion or disruption of services to the society's Internet line violets this policy. For example greeting card, video clip, sound or other large file attachments can degrade the performance of the entire network is an abuse of the system.

2.1.2 Downloading from the Internet/Online Services

Policy statement: The creation, download, viewing, storage, copying or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, fraud and other illegal activities using the Uganda Red Cross Servers either on site or remotely is highly prohibited.

Policy Penalty: Any user of the Uganda Red Cross Society ICT resources found involved in such an act is said to be abusing the system and therefore reliable to punishment by the disciplinary committee.

2.1.3 Pornography

Policy statement: Pornography is sexual material that leaves nothing to the imagination. The material is obsessed with sex and includes close-up shots of the actual or simulated sex acts. Therefore, the creation, download, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials using the Uganda Red Cross Internet line is illegal and prohibited.

Policy penalty Any breach of any of the above guidelines will lead to disconnection from URCS computer network and thereafter face the disciplinary committee for the appropriate punishment.

2.2 Email Usage Policy Guideline

Introduction: Electronic Mail and messaging systems are an increasingly important part of the Society's ICT strategy. Email systems are designed to enhance communication within the Society and beyond borders. It allows users communicate from their desk to various correspondents worldwide.

The Email Policy provides guidance about acceptable use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software and networks, provided by Uganda Red Cross Society . The Policy also describes the standards that users are expected to observe when using these facilities for email, and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

2.2.1 The main purpose of Email Services

The Main purpose for the provision by URCS of the ICT facilities for Email is for use in reporting, research, sending proposals, information sharing and other approved business activities of URCS.

Policy statement: All staff and volunteers of Uganda Red Cross Society email accounts must be in the official names that appear on the contract letters and academic documents. The use of company email systems from remote locations may create records of company activities that are not stored on equipment owned by the company. Therefore, unless the URCS email user is outside the country or in an inevitable circumstances remote usage of the URCS emails is not encouraged

2.2.2 Email Services Abuse

Therefore, ICT facilities provided by URCS for Email should not be used:

- 1) for transmission of unsolicited commercial or advertising material, chain letters, press release or other junk mail of any kind, to other user organizations connected to other networks other than where that material is embedded within or is otherwise part of the service to which the member if the user organization has chosen to subscribe.
- 2) for the unauthorized transmission on behalf of URCS to a third party of confidential information concerning activities of URCS
- 3) for activities that corrupt or destroy other users information/data
- 4) for activities that disrupt the work of others
- 5) for creation or transmission of information that either is discriminative or encourage discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, material status, disability, political or religious beliefs.
- 6) for creation or transmission of information that is abusive or threatening to others or serves to harass others
- 7) for criticizing individuals, including copy distribution to other individuals
- 8) for creation or transmission of anonymous messages i.e. without declare identity of the sender

2.2.3 Personal use of URCS Emails

The main purpose for the provision by URCS of ICT facilities for Email has been well defined in this policy. URCS permits the use of ICT facilities for email by staff and volunteers for personal use subject to the following limitations:

- o Personal use must not be of a nature that competes with URCS business activities

- Personal use must comply with URCS policies and regulations and in particular the email policy
- A level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided
- Personal use must not be for commercial or profit making nature or any other form of personal financial gain.
- For Email systems must not be used to infringe copyright, perpetrate fraud, distribute defamatory statements, and otherwise inflict harm on third parties. Because of the scope of this new medium, the harm caused by a wrongful message may occur more rapidly, or be greater in scope, than that caused by paper documents. Any use of the URCS email in such manner is an illegal act that reliable to disciplinary action.

Policy penalty: It should be noted that the use of URCS ICT facilities for email in unacceptable and inappropriate manner and breach of this policy would be treated as disciplinary offence.

URCS will investigate complaints received from both internal and external sources about any unacceptable use of email that involves URCS ICT facilities where there is evidence of criminal offence; the issue will be reported to the law enforcement body for the appropriate action. URCS will cooperate with this body and other external agencies in the investigation of the alleged offence.

Breach of the ICT regulation will lead to disciplinary action. Initially, this may involve a warning and an interview with the ICT specialist. Further disciplinary action depends on the severity of the offence and any previous instances by the person in question.

2.3 Office Computing Services Policy Guideline

Introduction: It is URCS policy to promote office computing in all her areas of operations for efficiency. In this context the term office computing is used for the application of ICT, mostly desktop computers, to support general office work. It does not only apply to clerical and secretarial work, but also to the office work of managers, heads of departments and officers. Office computing comprises a set of office-related functions in a single computer usually a desktop computer, either freestanding or linked to the Society's LAN. Major office computing applications are: Spreadsheets, word processing, electronic mail, desktop publications, graphics, presentation software and access to the Internet. To be effective, office computing not only requires appropriate computer systems, but also adequate knowledge skills in the use of the computer systems and various office applications. Therefore, a major component of the Society's ICT policy is the development of these general end-user computer skills.

2.3.1 Recommendable Office Applications and Operating Systems

All documentation and filing of the official documents such as reports, minutes of meetings, presentations, proposals etc should be done using the following Microsoft software products:

- ❑ Microsoft Word 2003+ for word processing
- ❑ Microsoft Excel 2003+ for spreadsheets
- ❑ Microsoft Power Point Presentation 2000+ for presentations
- ❑ Quark Express 5+, Microsoft publisher 2000+, Illustrator 7.0+, Photoshop 7.0+ for publications
- ❑ SPSS, EPIFO and stata for Data Analysis
- ❑ Microsoft Business Navision for Financial Management
- ❑ Microsoft Access 2000+, MSOL for Database Management Systems

- Microsoft Windows XP professional, Microsoft Windows Vista and Linux Fedfora for Operating Systems.

For all documentations that including report writing, minutes of meetings, proposals, monitoring and evaluations reports the following are the recommended formats:

Font Size: 11

Font: Verdana

2.4 ICT Security Policy Guideline

Introduction: URCS acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control.

Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

1. Confidentiality of Information.
2. Integrity of data.
3. Assets.
4. Efficient and Appropriate Use.
5. System Availability.

Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, as when a character in a file is altered.

The assets that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Power and Communications utilities.
- Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.
- Information.

Efficient and Appropriate Use ensures that URCS IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed "**threats**". These threats may be human or non-human, natural, accidental, or deliberate.

2.4.1 Reasons for URCS ICT Security

Policy penalty:

- a) The hardware and software components that constitute the URCS' ICT assets represent a sizable monetary investment that must be protected.
- b) The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.
- c) The use of URCS IT assets in a manner other than and for the purpose for which they were intended represents a misallocation of valuable Society's resources.

- d) Proper functionality of IT systems is required for the efficient operation of URCS. Some systems, such as the HRS and Finance are of paramount importance to the running of the National Society.

2.5 Physical security

Policy statement: All staff and volunteers are responsible for the physical security of all ICT equipments in their possession. Losing your computer means losing your fieldwork, reports, proposals, work plans, minutes of meetings, monitoring reports etc. Laptops are the easiest target for thieves - they can be easily put in a bag or carried away. Security precautions should be taken for any type of computer by URCS staff.

There are a few easy steps that can be taken to help minimize the risk and effect of physical security.

1. Do not leave your room accessible to anyone (open or unlocked door or window), even for a few minutes, when you are not there.
2. If you take you laptop with you in the car, lock it in the boot out of sight. Never leave it on the seat in full view.
3. If possible, carry your laptop in a non-descript bag or rucksack rather than an easily identifiable "laptop bag".
4. When not in use, lock your computer away, out of sight.
5. Keep a note of the serial number, make and model of your computer just in case.
6. To avoid un authorized access to your computer, ensure that you have a password on your computer both for opening the computer and screen saver password.

Incase there is any theft or physical damage to the National Society ICT equipment; the user will be responsible for its repair or replacement as the case maybe.

2.6 Network Security

2.6.1 Network General policy Guidelines

Introduction: Computer network is the inter-connection of computers aimed at sharing resources. URCS has installed a Local Area Network at the National headquarters. The following are the basic requirements of securing network resources:

Policy Statement:

- Ensuring that only authorized individuals have access to information
- Preventing unauthorized creation, alteration or destruction of data
- Ensuring that legitimate users are denied access to information
- Ensuring that resources are used in legitimate ways
- Ensuring that disaster recovery program is in place.
- Ensuring regular update of anti virus tools

While using the URCS computer network, the following should be strictly be observed

- a) All persons using the networking facilities shall be responsible for the appropriate use of the facilities provided and shall observe conditions and times of usage.
- b) It is the policy of the URCS that network facilities are not to be used for commercial purposes or non-URCS related activities without written authorization from the management. In any dispute as to whether work carried out on the networking facilities is internal work, the decision of the disciplinary committee shall be final.
- c) URCS endeavour to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect

the confidentiality of such information and material, but the URCS shall be under no liability in the event of any improper disclosure.

- d) If a loss of information within the system can be shown to be due to any hardware or software failure which is beyond the user's means to avoid or control, then the ICT unit will endeavour to help restore the information and will not charge the user of any case.
- e) Users of the computing networking facilities recognize that when they cease to be formally employees of URCS, their personal information may be removed from URCS networking facilities without notice. Users must remove their information or make arrangements for its retention prior to leaving the URCS.
- f) URCS reserves the right to limit permanently or restrict any user's usage of the networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the networking facilities; and to do so with or without notice to the user in order to protect the integrity of the networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.
- g) URCS reserves the right to take emergency action to safeguard the integrity and security of the networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of URCS take additional actions under this policy.

Policy penalty: The ICT unit may suspend any person from using the computing and networking facilities for a period not exceeding 28 days (and may recommend additional penalties to the disciplinary committee if after appropriate investigation that person is found to be: -

- o responsible for willful physical damage to any of the networking facilities;
- o in possession of confidential information obtained improperly;

- responsible for willful destruction of information;
- responsible for deliberate interruption of normal services provided by URCS computer network
- responsible for the infringement of any patent or the breach of any copyright;
- gaining or attempting to gain unauthorized access to accounts and passwords;
- responsible for inappropriate use of the facilities.

2.6.2 Restricted Software and Hardware.

Policy statement: Users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other Information which could result in the violation of any URCS policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers.

The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of URCS policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information.

2.6.3 Wasting Network Resources

Policy statement: It is inappropriate use to deliberately perform any act, which will impair the operation of any part of the networking facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

The willful wasting of networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using the networking facilities for the establishment of unnecessary chains of communication connections is an inappropriate waste of resources.

The sending of random mailings ("junk mail") is discouraged. It is bad and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and request to be removed from the mailing list.

Policy penalty: Whoever is found a victim of such circumstances is liable to disciplinary action which includes disconnection from the network among other things.

2.6.4 Online Game Playing

Policy Statement: URCS network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a on URCS network prohibit others who need to use the facility for official business activities.

Policy penalty: Therefore, online games by any staff or volunteer are an abuse of the network policy and a disciplinary matter.

2.6.5 Use of Mobile Computers (laptops)

Policy statement: Users are responsible for the security and integrity of URCS information stored on their laptop computer systems. This responsibility includes making regular disk backups, controlling physical and network access to the machine. Users should avoid storing passwords or other information that can be used to gain access to other URCS computing resources. Users should not store URCS passwords or any other confidential

data or information on their laptop or home PC or associated floppy disks or CD's.

2.6.6 Privacy of expectations

Policy statement: The URCS volunteers and employees do not have a right, nor should they have an expectation of privacy while using any URCS computer Network at any time, including accessing the Internet or using the Email. By using the Society's office equipment, employees and volunteers imply their consent to disclosing the contents of any files or information maintained or passes through the Society's network. However, electronic communications may be disclosed within a program or department to employees who have a need to know in the performance of their duties.

Policy penalty: Therefore, online games by any staff or volunteer are an abuse of the network policy and a disciplinary matter

2.6.7 Password Management

Policy guideline: Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of URCS's entire corporate network. As such, all staff and volunteers are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All system users must observe the following password guidelines:

- All system-level passwords (e.g., root, Administrator, admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships such as financial systems must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

All user-level and system-level passwords must conform to the guidelines described below.

Some of the more common uses of passwords include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - a) Names of family, pets, friends, co-workers etc.
 - b) Computer terms and names, commands, sites, companies, hardware, software.
 - c) Birthdays and other personal information such as addresses and phone numbers.
 - d) Word or number patterns like aaabbb, 12345, etc.

To create strong passwords use the following features:

- Use both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{ } [] : " ; ' < > ? , . /)
- At least eight alphanumeric characters long
- Words not in any language, slang, dialect, jargon, etc.
- Avoid personal information, names of family, your car name etc.

- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered.

2.7 Hardware Management policy guideline

2.7.1 Hardware Security User Guideline

Policy statement: ICT hardware must be treated with care and used only accordance with the proper operating instructions. No equipment shall be used which is labeled out of order. Any apparent fault with hardware should be reported promptly to the ICT unit. ICT equipment must not be used if there is reason to believe that it may not be in safe working order.

Users must not access and/or attempt to access any equipment, software and/or data which they are not properly authorized to access. In particular, the confidentiality of data belonging to other users must be respected.

Users must not by any deliberate or careless act or omission jeopardize or seek to jeopardize the integrity of any ICT equipment, and/or its software and/or any information stored within it and/or accessed through it.

Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use. Users must not use access codes that belong to someone else.

Users must not use any IT facility for a purpose other than that for which they are authorized. Users must seek advice if they have any doubt about their authority to use any of the ICT facilities.

Users of ICT must take all reasonable steps to exclude and avoid the spread of malicious software such as virus, worms, and must co-operate fully with the ICT unit to prevent the spread of such malicious software. In particular end-users of the hardware must not install any software obtained from a third party source or downloaded software, unless such software has been previously checked and cleared of the presence of malicious software by ICT

unit technical persons. Under the computer Misuse Act 1990, it is an offence knowingly to corrupt a computer program or any of the data stored in the computer system.

The use of any ICT equipment for storage and/or transmission of information which is considered to be obscene and/or offensive is strictly prohibited. Besides, ICT equipments must not be used to download pornographic, obscene, excessively violent and/or offensive materials from the Internet.

Computers programs on the ICT equipments are protected by law of copyright. URCS has appropriate licenses to use these programs, therefore ICT users must comply with the legal obligations concerning copyright and must not copy any software or other data without the prior authorization from the copyright owner. Such action would be a breach of copyright law.

2.7.2 Hardware Personal use

Policy Statement/guideline: URCS permits the use of its ICT equipments by staff and volunteers for personal use, subject to the following limitations:

- Personal use must not be connected to any purpose or application that conflicts with URCS rules, regulations, policies and procedures.
- Priority must be given to use of resources for the main purpose for which they are provided.
- Personal use must not be of a nature that competes with URCS business activities
- Personal use must not be commercial or profit making nature, including private consultancy, or for any other form of personal financial gain, unless prior written approval is obtained from management.

2.8 URCS Software Management and Usage Guidelines

2.8.1 Software License Management

URCS uses licensed Microsoft from recognized Microsoft recognized partners in Uganda. The software developer usually copyrights such software and, unless expressly authorized to do so, URCS has no right to make copies of the software. The purpose of this policy guideline is to prevent copyright infringement and to ensure proper software asset management.

It is the policy of URCS to respect and adhere to all computer software copyrights and to adhere to the terms of all Software licenses. It is also the policy of URCS to manage its software assets and to ensure that it installs and uses only legal software on its desktop computers (including portables) and servers.

URCS will take all steps necessary to prohibit its users from duplicating any licensed software or related. Documentation for use either on URCS premises or elsewhere unless it is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software URCS staff and volunteers is prohibited and tantamount to disciplinary action.

It is the URCS policy to acquire, copy, distribute, transmit and use software in accordance with the policies of the Society and the terms and conditions in any license agreement accompanying that particular product.

2.8.2 Software Acquisition

Policy statement: Legitimate software must be provided to all system users who need it. All requests for software including upgrades must be submitted to the ICT unit. All software acquired by URCS must be approved

and purchased through the ICT unit. Software must be purchased only from reputable, authorized software vendors.

Software must not be purchased through petty cash. If software is acquired through other means for example given free by implementing partners, the ICT unit should be notified for documentation purposes.

Software acquisition channels are restricted to ensure that URCS has a complete record of all her software that has been purchased for and can register, support, and upgrade such of software accordingly.

2.8.3 Software Installation

Policy guideline: After the legal acquisition of the Society's software as described the following installation guidelines must be observed.

1. Only personnel from the ICT unit are recommended to carry out software installation on the Society's computers, laptops and the network.
2. Only those persons explicitly authorized by URCS to install software may install software on organization's computers and servers. Such persons shall not do so unless and until URCS has first obtained an appropriate license for that software.
3. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

2.8.4 Storage of Software and Documentation

Policy guideline: Once installed, the original media will be kept in a safe storage area maintained by the designated department. The designated department will also store all original software licenses and registration and purchasing information in a safe storage area. User manuals, if provided, must reside with the ICT but may be loaned to users if the ICT unit keeps

records of who has borrowed the manual. The ICT unit shall destroy all copies of software that are obsolete or that organization is no longer licensed to use.

The ICT unit shall keep and maintain a register of all organization's software. The register must contain:

- a) the title and publisher of the software
- b) the date and source of Software acquisition
- c) the location of each installation
- d) the software product's key number.

2.8.4 Using Company Software on Home Computers

Policy Guideline: URCS computers are organization-owned assets and must be loaded with only legal software. Only software purchased through the procedures outlined above will be used on URCS machines. Users are not permitted to bring software or other copyrighted material from home and load it onto URCS' computers. Also URCS-owned software cannot be taken home and loaded on a user's home computer. The employee is to use software at home, if the software company provides License agreements that home use is permitted. If an employee needs to use software at home, he/she should consult with the ICT unit.

2.8.5 Software Audits

Policy Guideline/statement: URCS reserves the right to inspect an employee's computer system for violations of this policy. The ICT unit will conduct a regular audit of all URCS' computers (including portables) and Servers, to ensure that organization are in compliance with all software licenses. Periodic, random audits shall also be Conducted as appropriate. Audits will be conducted in a manner that is the least intrusive and disruptive to the staff. The full cooperation of all users is

required during audits. Employees must not remove or delete the software. The removal or deletion of software must be done only by the ICT unit or authorized party by the management.

2.8.7 Discipline

Policy Penalty: Any URCS staff that becomes aware of the installation, copying, use, distribution, or transmission of software within this organization that is illegal or conflicts with organization's software management policies shall promptly notify an appropriate person. This may include his or her supervisor, ICT unit or an appropriate employee within the organization. Any infringing activity by an employee may be the responsibility of the organization. Therefore, URCS may choose to hold the staff or volunteer liable for their actions.

3.0 Identified ICT Services and Information Systems

The society's ICT policy anticipates the implementation of the following ICT services and information systems as well as related implementation, operation and management issues.

- Internal and external E-mail and access to Internet services at all workplaces embodying office internal and external communication through Internet/Email technology.
- Availability of common office applications such as word processing, spreadsheet, Desktop publishing, Graphics, Presentations, Databases at all work places.
- Integrated Financial Information System
- Integrated Human Resource Information System
- Integrated Membership Management System
- Tracing Information Management Systems
- Geographical Information System (GIS)

It is assumed that the facilitation of all the above ICT systems and services is the responsibility of all departments. It is also party of the society's policy to;

- Sustain management of ICT resources through the creation of appropriate policy, advisory management and operational organs that will cater for the broad interest of all users.
- Implementation of a reliable ICT disaster recovery security system by providing backup servers for data and Emails.
- The society's ICT policy has provision for promoting office computing in all offices. In this context, the term office computing is used for the application of ICT, mostly desktop computers and related accessories to support general office tasks both at the headquarters and branch level. This applies to management staff, program heads, program officer, administrative officers and volunteers.

- It is the society's ICT policy to ensure that all staff; managerial, head of departments and officers both at the headquarters and branch level are trained on continuous basis to equip them with the requisite skills to fully exploit the ICT environment in their different functions.

4.0 End User Skills Development

4.1 Human Capacity Development

In an environment where administrative and managerial processes are automated, the necessary skills to utilize the services/systems, keep them running and implement them demand new and high-level skills.

It is the Society's ICT policy to promote the deployment of ICT in all programs both at headquarters and branch level in the broadest sense. The Society needs to ensure and requires that all staff be trained on a continuing basis to equip them with adequate skills to fully exploit the ICT environment in their different functions.

End-user skills development includes all efforts to enforce awareness, general knowledge and specific computer skills related to the use of information technology. Within this context, the end user is defined as each person who uses ICT services to enhance on his/her daily office work.

Knowledge and skills for the development and implementation of ICT services and systems is very limited countrywide. As a result, staff training in use of ICT services and system, development of ICT professional skills should be given high priority goals of the Society's ICT policy.

In line with the implementation of different ICT services and systems considerable knowledge and skills have to be developed among the end-users so that they are empowered to;

- Use ICT service and systems effectively and as independently as possible
- Establish and sustain effective, efficient application and data management and system maintenance

- Be aware of the shared responsibilities for equipment, software and data and enforce an atmosphere of collective responsibility and system ownership.
- Contribute to the specification, design and implementation of IT applications.

The URCS IT policy provides for the development and implementation of a consistent set of training programs with different categories of ICT users. These include among others management staff, head of departments, program officers, administrative assistants and contract volunteers.

Training should be provided to cover, as far as possible all skill levels. While it is not intended to turn all users into experts, it is important that the training plan supports all users of ICT at all levels. The short- and medium-term goals shall aim at creating, as rapidly as possible, a sizeable proportion of staff that are familiar with and are able to effectively use the ICT infrastructure in their daily work. At the end of the training, URCS expects that:

- All staff at all levels are able to use standard application packages (Word, Excel, Power Point, Publisher, Access) as well as Email and Internet with ease.
- Administrative chores such as calling meetings and distribution of minutes and other documents are handled via e-mail.
- All official corresponds via e-mail be handled using the URCS email accounts for respective programs.

5.0 Policy Implementation

5.1 Role of senior management

The success of any ICT policymaking exercise is dependant on obtaining approval and support from top management, whose commitment will enable an organization to establish a cohesive link between the organization's objectives and policies of ICT. Top management commitment must ensure that ICT policy decisions are driven by real ICT needs and the desire to improve the Society performance. Top management must foster a climate in which innovation through ICT can develop.

Direct and active participation from senior management should be a continuous process. Taking into account the substantial impact on operational and managerial processes and funds needed to develop and sustain the ICT.

5.2 User responsibilities

To assist in the orderly implementations of ICT services and grow in an understanding of their use, cost and impact on the Society, the potential users of ICT services should fulfill the following responsibilities;

1. Clearly understand the scope of all ICT services supporting the user.
2. Permitted limited use of the society ICT equipments for personal needs if the use does not interfere with official business and involves minimal additional expense to the National Society in areas such as;
 - a. Communication infrastructure costs e.g. telephone charges, telecommunication traffic etc.
 - b. Use of consumables in limited amount e.g. paper, ink, toner etc.
 - c. General wear and tear on equipment
 - d. Data storage on storage devices such as floppy diskettes, CDs etc.

- e. Transmission impacts with moderate email message sizes such as emails with small attachments.

5.3 Implementation Team

The Society has decided on the following general policies for the development of appropriate Information Resource Management capabilities.

Implementation Committee

An ICT Implementation Committee will be established, providing a high level, mechanism to:

- o Monitoring and control the progress of all activities arising from the implementation of the URCS' ICT policy
- o Recommend proposals for cost-recovery and cost-sharing
- o Determine/approve ICT policy adjustments arising from technology trends or new strategies.
- o Budget for the cost of management, operations, maintenance and expansion of the Society's ICT at all levels
- o Allocate ICT resources according to the agreed plan

Members of this committee should be head by the Deputy Secretary General and comprised of the following: -

- o Head of Internal Auditor
- o Head of Logistics and procurement
- o Head of Disaster Management
- o Head of Planning, Monitoring and Evaluation
- o ICT Coordinator
- o Head of Finance and Accounts