ICT Handbook

Government of the Republic of Liberia

Monrovia, Liberia

Title:	**ICT Handbook**
Date Adopted:	**June 26, 2015**
Originating Office:	**Ministry of Posts and Telecommunications**
Distribution:	**All GOL Ministries, Agencies & Commissions**

MESSAGE FROM DR. FREDERICK B. NORKEH, MINISTER,

MINISTRY OF POSTS AND TELECOMMUNICATIONS

It brings me great pleasure to present the National ICT Handbook which is geared toward providing guidance to the use of ICT facilities by Public Officials and Civil Servants in the Government of Liberia. As the use of Information and Communication Technology (ICT) facilities is significant to facilitate efficiency, reliability and transparency in public offices, it is important to guide against the misuse of this technology. In 2006, the Government of Liberia and in particular, the Ministry of Posts and Telecommunications was faced with enormous challenges around the development of ICT in Liberia. The Telecommunications sector of Liberia was hugely underdeveloped with the consumers bearing the burden of the cost for the use of technology. Cybercafés were very scarce, and computer technologies that facilitate job efficiency, reliability and transparency were limited in government ministries, agencies and commissions. The scarcity of ICT facilities and cost implications for consumers generated the need for reform.

The Government of Liberia, at this point in time, prioritized the liberalization of the sector to ensure competition. Interestingly, internet service providers were struggling to provide services to subscribers via satellite which instils an additional cost on consumers. To date, the reform has yielded several benefits for not only service providers but consumers alike. Many consumers are currently having easy access to information and other social networking platforms through the use of internet; while service providers are now incurring lower cost for service provision than before.

Notwithstanding, it is also important to note that the safe landing of the "African Countries to Europe" (ACE) submarine cable (Liberia's first fiber optic cable) in November 2011 served as a gateway for the provision of fast internet services. This part of the reform was as a result of a collaborative effort amongst key players in the ICT sector of Liberia; to include: the Government of Liberia, Liberia Telecommunications Authority, Liberia Telecommunications Corporation, Cable Consortium of Liberia, and other Private Service Providers (Lonestar/MTN, Cellcom and MTN).

Essentially, as we endeavor to use ICT to facilitate growth and development, it is incumbent upon us as policy makers to guide against the misuse of ICT facilities in ministries, agencies, and commissions. If we should succeed as a government in using ICT facilities to enhance efficiency, productivity and proficiency, line ministries, agencies and commissions must adopt and ensure strict adherence to this working tool which encompasses the do(s) and don't(s).

At this juncture, I crave the support of all heads of agency, ministry and commissions in ensuring that individuals within their employ use the technology wisely and avoid misuse as advised by the National ICT Handbook. This fight is not for us alone, but for all well-meaning Liberians in public places that deem it expedient to provide protection against misuse of government equipment during working hours. This is one of the new challenges in the sector that, we as a people and country must seek to address. This handbook is the first step, and your adherence is the next.

FB norkeh

Dr. Frederick B. Norkeh

Minister/Postmaster General - Ministry of Posts and Telecommunications, RL.

Table of Contents

GoL Staff Intranet, Internet and Electronic Mail Usage Handbook

Purpose:

The purpose of this handbook is to define and outline authorized use of Internet, email and other ICT facilities and devices. The policy applies to all users of government-owned ICT resources (including government staff and any third parties), hereafter referred to as 'authorized users' or 'Government of Liberia (GOL) staff.'

This handbook should be read in conjunction with related MAC standards, codes of conduct, and laws and regulations of the Republic of Liberia.

This handbook comes into effect on 26 June 2015

1. Policy Statement

The intranet, Internet and electronic mail (email) are important business, teaching and learning tools that can enhance workflow, increase productivity and help GOL staff perform a variety of tasks. As such they should be used in an efficient, lawful and ethical manner.

GOL staff are accountable to senior management for appropriate use of these technologies and are required to abide by this Intranet, Internet and Email Usage Policy.

2. Scope

1) This handbook serves as a guide to what constitutes acceptable behavior when using GOL ICT resources. It identifies the principles for the access to and proper use of intranet and Internet services; the receipt, review and disclosure of email messages; and the proper use of email services provided by GOL ministries, agencies, commissions, or MACs.
2) This policy applies to:
    i) All GOL ICT facilities and devices (including intranet, Internet and email services) that are owned, leased, or utilized by the Government, regardless of their location.
    ii) All GOL staff, regardless of location, who utilize, support or manage these ICT resources, including:
        (1) Permanent, temporary and seconded staff
        (2) Contractors and consultants
        (3) Students, volunteers, and interns
        (4) All other external bodies who are authorized by the MAC to use government ICT facilities and devices
        (5) Any other third party
3) This document is not comprehensive, but rather it provides guidance for authorized users and managers to exercise a common-sense, reasonable approach in the use of ICT facilities and devices. It may be updated as deemed necessary, in accordance with GOL rules and regulations.

3. Objectives

a) The objectives of this policy are to:

i) Address issues of compliance with existing government information standards, including the Freedom of Information Act.

ii) Protect staff by informing them of the rights and responsibilities associated with use of intranet, Internet and email services;

iii) Prevent misuse of MAC assets;

iv) Protect the MAC from legal liability;

v) Ensure optimal network bandwidth and ICT resources for all authorized users to perform work-related function;

vi) Protect intranet, Internet and email services from attacks and outages;

vii) Protect against loss of information;

viii) Ensure capture and retention of government electronic records.

b) This policy cannot be totally exhaustive. Where situations not covered by this policy arise, GOL staff should contact senior management for further guidance.

4. Usage of this document

a) All GOL staff who utilize, support or manage government-owned or leased intranet, Internet or email services should be aware of this policy, which includes their responsibilities and legal obligations.

b) Before a new user is authorized to access GOL ICT resources, they will be required to sign a copy of the GOL Staff Intranet, Internet and Electronic Mail Usage Policy, indicating that they have read and understood the policy and accepted the terms and conditions.

5. Compliance

a) All GOL staff are required to comply with governmental policy and are bound by law to observe applicable statutory legislation relating to personal data, company data, public records, copyright and other forms of intellectual property and misuse of information and facilities.

6. Accountabilities

a) Intranet, Internet and email access is provided for officially approved purposes only, i.e. MAC business and limited personal use, as defined below.

b) GOL staff must comply with all policies, legislation and regulations applicable to the use of the intranet, Internet and email.

c) Intranet, Internet and email usage should be able to withstand public scrutiny and/or disclosure, as required under any related legislation. Unauthorized access, transmittal or storage of material that might bring the GOL into disrepute is prohibited.

d) 6GOL information should not be transmitted or made available via the intranet, Internet or email except under government-approved protocols.

e) GOL staff should not use the intranet, Internet or email in a way that could defame, harass, abuse or offend other individuals or organisations.

f) GOL staff should not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, malicious or pornographic material, as defined in Appendix I of this policy.

g) GOL staff should not disrupt or interfere with the use of intranet, Internet or email services.

h) Authorized users will be granted a network account and password, and must not knowingly permit another person to use their network account or enable another person to access ICT resources, such as the Internet, without authorization.

i) GOL staff should not attempt any unauthorized access of intranet, Internet or email services. Unauthorized access includes, for example, the distribution of messages anonymously, use of other officers' user IDs or using a false identity.

j) GOL staff should not damage, delete, insert or otherwise alter information carelessly or with malicious intent.

k) GOL reserves the right to monitor and audit any or all intranet, Internet or email activity undertaken by GOL staff using MAC resources. GOL staff may be called on to explain their use of the intranet, Internet or email.

l) Email and electronic files are subject to record keeping, archiving, Freedom of Information and legal process. As such, emails and files created using GOL ICT resources should not be regarded as private, unless otherwise exempted in accordance with GOL law and regulations.

m) Violations of MAC policy may result in restriction of access to technologies, disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

7. Staff Responsibilities

a) All GOL staff are expected to take reasonable precautions to protect intranet, Internet and email information and systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.

b) The following guidance is provided of activities that constitute Acceptable Use of ICT Resources and those that constitute Unacceptable Use of ICT Resources.

Acceptable Use of ICT Resources:

c) The intranet service, which allows users to easily share information within an institution, can only be used for MAC business purposes.

d) Internet and email services are also intended for MAC business use. However, limited professional and personal use may be permitted, in accordance with the guidelines described below.

e) Official Business includes any activity that is conducted for purposes of accomplishing official work activities. Examples include:

   i) Using ICT facilities and devices for work-related activities;

   ii) Using the internet to access work-related information;

   iii) Sending emails to colleagues on work-related matters; and

   iv) Sending emails outside of the work environment on work -related matters.

f) Professional duties include:

  i) Using the internet for professional development such as approved study, research or professional forums;

  ii) Limited use of computer, email and other ICT facilities to support study; and

  iii) Limited support for staff to engage with professional associations.

g) In general, ICT use for professional development should be approved in advance by senior management, and done in an employee's own time. It should not interfere with work activities or affect the productivity of other employees.

  i) Limited personal use means use that is infrequent and brief. It includes:

  ii) Limited personal emails and internet searches that are not unauthorized, unlawful or criminal;

  iii) Using a printer or photocopier to print out a few pages of personal information;

  iv) Sending emails collecting for charities, school raffles and similar activities;

  v) Making financial transactions including bill paying or home banking;

  vi) Accessing Internet news, articles, and social media (including Facebook and twitter), assuming they do not require excessive bandwidth;

  vii) Purchasing non work-related goods and services;

  viii) Booking holiday accommodation and personal travel; and

  ix) Using personal email to send non work-related messages.

h) Individual staff will be held personally responsible for any use of intranet, Internet and email services that does not comply with these principles.

Unacceptable Use of ICT Resources

i) Under no circumstances are MAC employees authorized to engage in any activity that is illegal under Liberian law while utilizing Government-owned ICT facilities and devices. Illegal and unauthorized activities include the use of ICT resource to:

  i) Download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity or religious and political beliefs.

  ii) Download information for the purpose of providing it to external organisations or the general public without authorization.

  iii) Excessively use MAC ICT resources for personal use or non-work related activities, such as private business or personal profit ventures.

  iv) Engage in any illegal or wrongful activity, store unlawful information, or otherwise use MAC ICT resources in ways that violate local or international laws or statues.

  v) Change or view any electronic document where the author or owner has not permitted such activity.

  vi) Circumvent security measures on MAC ICT devices or networks.

  vii) Vandalize ICT resources, which is any malicious attempt to harm or destroy data or equipment of another computer user.

j) When sending and receiving messages, the following will be viewed as unauthorized use of ICT resources:

  i) Sending or receiving materials that are copyrighted by the MAC or third parties without permissions.

  ii) Using impolite, abusive, or otherwise objectionable language in public or work-related communications.

  iii) Distributing defamatory, obscene, offensive, or harassing messages.

  iv) Distributing confidential information without authority.

  v) Distributing messages that disclose personal or private information without authorization.

  vi) Sending messages or sharing information resources infected by malicious codes, such as viruses.

  vii) Distributing messages anonymously, using a false identity or using another person's email account.

  viii) Emailing chain letters, pyramid schemes, or other such “get rich quick” messages, or any other type of mass mailings that would congest MAC ICT resources or otherwise interfere with the work of others.

  ix) Forwarding MAC business emails to external parties (including other government agencies) from a personal email account.

k) When accessing the internet, GOL staff must avoid the following unauthorized activities:

  i) Access, download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet sites.

  ii) Download software, unless they receive appropriate authorization and comply with licensing requirements and established policies to check all such software for computer viruses.

  iii) Stream videos (such as on youtube) or music, download large files, or otherwise excessively use shared bandwidth in such a way that hinders others’ ability to conduct work activities via the internet.

  iv) Attempt to gain access to another’s resources, programs, and data without proper authorization.

  v) Without authority destroy, alter, or prevent rightful access to or otherwise interfere with the integrity of intranet, Internet or email services.

  vi) Access inappropriate Internet sites, including:

    (1) Gambling sites

    (2) Dating sites

    (3) Sites that are illegal

    (4) Sites that are pornographic or contain inappropriate adult sexual material

    (5) Sites that advocate hate/violence

    (6) Sites that offer inappropriate games or software

  vii) Use the Internet to create or maintain personal websites, to run private ventures, or to excessively access social media (Facebook, twitter, etc.) for personal purposes.

l) The items above should not be considered comprehensive. Other inappropriate actions not listed may also be considered irresponsible and unacceptable use of GOL computers, networks, communications equipment, and ICT resources.

8. Password Policy and Security

a) Passwords are a very important aspect of computer systems security, and are typically the first line of protection for user accounts. A poorly chosen password may result in a serious breach in network and systems security.

b) GOL staff, including all contractors and guests who use the GOL ICT resources, are responsible for taking steps to select and secure their passwords.

c) Passwords are assigned to individuals for their own use. They should not be disclosed or shared with anyone other than authorised systems personnel. Sharing of passwords is a breach of policy by both the person providing the password, and the person receiving the password.

d) Passwords often assign system rights and system privileges to a user. These system rights and system privileges are assigned by authorized systems personnel, and no other attempts should be made to alter or change these rights. All passwords are to be treated as sensitive, confidential GOL information.

Password Do's and Don'ts

<u>Don't</u>

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to the boss.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on holiday.
- Don't use the "Remember Password" feature of applications (e.g., Web browsers, OutLook, etc).
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.

<u>Do</u>

- If someone demands a password, refer him or her to this document or the IT Systems and Network Administrator for advice.
- Change passwords at least once every four months.
- If you suspect that one of your accounts or passwords has been compromised then you must report this immediately to the IT Department, and change all your passwords.
- Refer to **APPENDIX II: General Password Construction Guidelines**

With thanks to the University of Glasgow

9. Email and Security

a) GOL staff who are assigned individual GOL email addresses and mailboxes should use these whenever possible to communicate in their work capacities. This will promote professionalism and standardization across the department, and will help ensure copies of all work correspondence are archived.

b) GOL staff who are not assigned individual GOL email addresses and mailboxes are encouraged to establish a dedicated account for work-related email using services such as Gmail or Yahoo. The ICT Unit will provide assistance.

c) Business-related email messages, whether sent from a GOL-assigned email account or a personal account in the case where assigned email accounts are unavailable, must have the user's name associated with the message. Anonymous work-related messages are prohibited.

d) GOL email messages are neither personal nor private. While the ICT Unit will not routinely monitor individual email and will take reasonable precautions to protect the privacy of email, program managers and technical staff may access an employee's email, on the authority of senior management:

   i) For a legitimate business purpose (e.g., the need to access information when an employee is absent).

   ii) To diagnose and resolve technical problems involving the system.

   iii) To investigate possible misuse of email when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

e) Some departments may require that a standard footer be appended to the end of each outgoing mail message that includes GOL or MAC branding, contact details and legal disclaimers. Senior management will inform GOL staff if a footer is required; if so, authorized users should take care to ensure that the footer is included in all official email correspondence

f) Refer to **APPENDIX III: Additional Guidance for Email Security and** Use and **APPENDIX IV: Best Practice Procedures for Sending Business Emails**.

g) This document does not attempt to be a comprehensive guide to the use of email.

10. Network Security

a) Only authorized software may be installed on government ICT devices. The ICT Unit will advise what software is authorized. Approval for all software installations should be granted by the ICT Unit Head before the installation. Great care should be taken not to install illegal software on the network.

b) Information contained on portable computers/devices is especially vulnerable and special care with respect to security must be exercised.

c) All computer desktops and server hosts used by staff that are connected to the MAC intranet or internet shall be continually executing approved virus-scanning software with a current virus database.

d) Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, Trojan horse code or any malicious code.

11. Computer Resources - A Finite Resource

a) GOL officers are reminded that computing resources are finite and are under increasing demand. An authorized user's use of ICT facilities should not interfere with or cause difficulties for other users.

b) Staff should take great care to minimize the use of the internet for non-work purposes. Every attempt should be made, even while pursuing work activities, to minimize the volume of data that needs to be transferred via the internet by avoiding the transfer of films, videos, sound and music files, high resolution graphics, software installation images, photographs and very large datasets.

c) Special needs should be brought to the attention of the ICT Unit who will advise on how best to proceed.

12.Social Media

a) Social media networks are a growing industry that encompasses a variety of online activities which are open to public viewing that is traceable. Social Media may include:

i) Social networking sites (eg Facebook, Myspace, LinkedIn)

ii) Video and photo sharing websites (eg Flickr, Instagram, Youtube)

iii) Blogs, including corporate blogs, media outlet blogs, and personal blogs

iv) Micro-blogging (eg Twitter)

v) Wikis and online collaborations (eg Wikipedia)

vi) Forums, discussion boards and groups (eg Google groups)

vii) Podcasts

viii) Online multiplayer gaming platforms (eg World of Warcraft, Second life)

ix) Instant messaging (including SMS, gchat, Facebook chat)

b) The rules and guidelines for use of the Internet and email also apply to the use of chat facilities and social media. Additional rules are provided below:

i) Staff are personally responsible for content published and comments left on social media websites. Staff are reminded that these views could remain in the public domain for a considerable length of time.

ii) Outside of the workplace, staff have the right to privacy and freedom of speech on their personal social networks. However, what staff publish on such personal online sites should never be attributed to the GOL, to any staff person, or to any client, and should not infringe upon confidentiality and privacy.

iii) Staff should be careful not to imply they are authorized to speak as a representative of the Government, nor give the impression that the views they express are those of the MAC or the Government.

iv) Staff should not use their MAC email address, nor government logos or insignia when posting on social media for personal reasons.

v) Social media should not be used for complaints relating to the GOL and/or the work place, as there are formal processes in place for complaints.

vi) Social media should not be used to respond to any negative, false, inaccurate or accusatory comments by another person.

vii) Photographs of the workplace, or of colleagues engaged in work or non-work activities at the workplace, should not be posted on social media without approval from senior management

c) GOL staff must obtain prior approval from senior management to engage in social media as a representative of the department. Staff may not comment as a representative of the MAC unless authorized to do so.

d) Authorized staff must abide by MAC protocol for ensuring approval of all material shared via social media.

Social Media Guidelines

<u>When using social media for personal use, consider the following:</u>

- Could what you are doing **harm the reputation** of your agency or the state?
- Are you disclosing any agency material that you are **not specifically authorized to disclose**?
- Have you made it clear to others when your contribution is as a private individual and **not as a representative of your agency**?
- Are you willing to **defend what you post** to your manager? Would you be comfortable saying it to a stranger at a bus stop, or posting it on a public shop window?
- Are you using **government-owned infrastructure**? Do you have permission to use it in this way (this includes the use of your government email address)?
- Are you behaving with **integrity**, **respect** and **accountability**?

<u>When using social media for personal use, consider the following:</u>

- Before engaging with a specific social media channel, ensure you understand its conventions and etiquette.
- When you are speaking on behalf of your agency, identify yourself as such.
- Correct any factual inaccuracies you find relating to government policy.
- Where users ask questions about policy or published information with which you are familiar, provide answers to the queries.
- Refer people to government sites, where appropriate.
- Ensure that any comment you make on matters of government policy is appropriate to the agency role you hold, and remains politically neutral.
- Do not give out personal details of yourself or other staff.
- Do not post any material that is protected by copyright.
- Abide by MAC protocol for ensuring approval of all material shared via social media.

With thanks to the Code of Ethics from the South Australia Public Sector, Commissioner for Public Employment Office of Ethical Standards and Professional Integrity, February 2010, page 13.

13.Services for which a Subscription Fee is Charged

a) There are many services available through the Internet on a user-pays basis. Where a GOL staff member identifies a service that is relevant to their official work duties, an application to subscribe to the service should be made through the Unit ICT

b) Under no circumstances should a GOL staff member enter into any subscription contract or agreement without the prior approval from senior management.

14.Confidentiality

a) All staff are expected to respect and safeguard all aspects of information confidentiality. Staff are expected to treat all MAC information, whether paper-based or electronic, as confidential. No one is permitted to disseminate MAC information outside the MAC without specific authorization from the author or management.

b) Refer to senior management (perhaps designate a position) or your department's Information Officer for more information on confidentiality and disclosure of official information.

15. Capturing and Accessing Public Records

a) As defined by the Freedom of Information Act of 2010 (FOIA), Section 1.3.12, a "Public Record means a record, manual rule book, regulation or other documents produced or received by, being used or having been used by, possessed by or under the control of a public authority, whether in written form or recorded or stored in electronic form or in any other device."

b) Under FOIA, public records may be subject to external scrutiny or required to be made available upon request from the public.

c) Email messages created, received or stored by staff in the conduct of or in connection with governmental business are deemed to be public records within the meaning of FOIA.

d) Under "Chapter 2.0: Publication of Certain Information" of FOIA, public authorities are obliged to publish certain classes of documents and information as soon as they are generated. Senior management or the MAC Information Officer will provide further guidance for ensuring staff are in adherence with FOIA requirements.

e) Emails (whether personal or business related) may also be tendered in court as evidence and are subject to legal processes such as disclosure and subpoena.

f) Per Chapter 3.0 of FOIA, an Information Officer should be appointed to each public authority with the responsibility to receive requests and, maintain, store and manage records, and assist the public in filing requests for information. Staff should consult this Officer or, in their absence, senior management for further information on FOIA requirements and the release of public records.

16. Privacy of email messages

a) Staff are not guaranteed privacy in relation to email messages sent using GOL ICT facilities and devices, whether the messages are business-related or personal. The reasons for this include the following:

   i) Email is not secure, unless it has been encoded or encrypted.

   ii) Email messages are hard to destroy. Email messages are backed up on a regular basis and can be recovered from these back-ups. The deletion of an email message from the email account does not remove the backed-up copy.

   iii) Email messages are logged. These logs include email sender and recipient addresses, time of transmission and the content of the email. These logs are necessary for routine maintenance and management of the email service.

b) The MAC respects the right of staff to privacy, but the MAC reserves the right to access GOL staff email messages under certain circumstances, as defined immediately below and in Section 18: Monitoring and Inspection.

c) The MAC may seek to gain access to an authorized user's email messages, in the same way as for paper-based material, where this is necessary for the purpose of retrieving business information or for system maintenance.

d) In the case of system maintenance, the extent of access will not exceed the minimum essential for the performance of the maintenance function.

e) In the case of access to retrieve business information, the authority of senior management is required before access is attempted, and the extent of access is restricted to no more than is necessary to locate and retrieve the relevant information.

f) Because it is a part of their official duties, a limited number of Information Officers, as designated under FOIA, have ongoing management authority to access and retrieve records created by GOL staff.

17.Copyright

a) Ownership of material. Documents, messages, email and correspondence created, received or stored using the department's ICT facilities and devices, are at all times, the property of the Republic of Liberia.

b) Copyright is a legal recognition of ownership of intellectual property, etc. Copyright laws protect most documents and software available through the Internet. GOL staff should consider the copyright implications associated with copying or otherwise reproducing Internet material.

c) It is prohibited to use the Internet service or email system to copy, reproduce or transmit any document, software or other information protected by copyright laws. This includes the download of pirated movies or music files (via sites such as Pirate Bay), as well as the usage of non-licensed software such as Word.

d) Officers should refer to the ICT Unit for further information on digital copyright.

18.Monitoring and Inspection

a) GoL reserves the right to monitor any or all Internet or intranet related activity and to monitor and inspect any or all email messages sent or received by GOL officers using MAC resources, in order to:

   i) Identify inappropriate use;

   ii) Protect system security;

   iii) Maintain system performance;

   iv) Protect the rights and property of the department;

   v) Determine compliance with GOL and MAC policy;

   vi) Determine compliance with GOL legislation and regulation.

b) Authorized users shall have no expectation of privacy in respect to their personal use of Internet, email and other ICT facilities and devices; however, using ICT facilities to collect, use or disclose personal information of others is subject to whole of government and MAC privacy standards.

c) These monitoring and inspection activities include but are not limited to the following:

   i) Access and examination of specific types of messages e.g. large messages or messages containing executables, audio visual files, movie files, command files and/or pictures, in order to identify inappropriate use or to maintain system performance;

   ii) Access and examination of messages in specific circumstances, such as where an individual's message volume is high, in order to identify inappropriate use or to maintain system performance;

   iii) Access, examination and referral of email messages for the purpose of complying with investigation requests received from law enforcement;

   iv) Access, examination and referral of email messages for good cause or to satisfy legal obligations, in compliance with legislative requirements and governmental policies. Good cause includes the need to protect system security, identify inappropriate use and protect the rights and property of the department;

   v) Introduction and use of content security software to protect GOL staff and the department's computer network, systems and services from such things as viruses or offensive material and breaches of confidentiality.

d) Filtering tools may be used to restrict access to certain categories or internet websites that have been deemed to be unauthorized; may have the potential to compromise the network through excessive downloads; or may be a threat to network security. The purpose of filtering is to protect authorized users and the MAC from accidental access to sites that may contain unauthorized material.

e) Automated tools may be used to scan and block email messages and attachments that may contain unauthorized content; viruses or other codes that might be harmful to the network; large files (such as movie files); and spam.

f) If an email or website is blocked, the intended recipient may request the ICT Unit to release the information if it is deemed safe, and is related to the organization’s work activities.

19. Consequences of Policy Violations

a) GOL staff use of intranet, Internet and email services should be compliant with the principles and expectations laid out in this policy and, where applicable, the MAC Code of Conduct and related standards and regulations.

b) Violations of this policy may result in restriction of access to intranet, Internet and/or email services and may lead to disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

c) Staff who are aware of, or observe a suspected violation of this policy, are responsible for reporting the incident to their supervisor.

20. Ongoing Development

a) It is intended that this policy continues to develop so that it keeps pace with MAC requirements and the progress of information technology. Requirements, suggestions and comments about these documents should be forwarded to senior management.

21.Responsibility

a) Control and Administration. The Chief Information Officer/RL is responsible for the control and administration of this policy document.

b) Compliance. All GOL management (Directors and above) are responsible for ensuring that this Intranet, Internet and Email Usage Policy is observed.

c) Awareness. Workplace managers are responsible for ensuring that all GOL staff associated with their area are made aware of this policy.

22.Contact

For further information contact:

Chief Information Officer (CIO), Ministry of Posts and Telecommunications

APPENDIX I: Definitions

Authorized use: Use of Internet, email and other ICT facilities and devices for purposes directly related to business of the MAC or for limited personal, educational or self-development purposes.

Authorized user: Those persons who have been approved to access the MAC computer network in accordance with MAC policies and standards.

Chat: Talking to other people on-line. There are many forms of chat including chat lines, chat groups, chat rooms, and discussion lists. Some commonly used examples are Google's gchat and Facebook chat.

GOL staff: Refers to all GOL permanent, temporary, seconded or contracted staff and consultants. Volunteers and interns who assist staff with their professional duties and utilise MAC intranet, Internet and email services are also classified as GOL staff for the purposes of this policy.

Email messages: A computer-based message sent via the communication network to one or more recipients. An email message may be transmitted with one or more attachments i.e. files containing text, graphics, images, digitised voice, digitized video or computer programs.

Firewall: A method of protecting a network against security threats from other systems and networks by centralising and controlling access to the network using a combination of hardware and software controls.

Integrity: Sound, undiminished and unimpaired condition.

Internet: The Internet is a worldwide loose affiliation of interconnected computer systems, through which users can navigate to obtain services and share information with globally dispersed organisations and individuals.

Intranet: The intranet is essentially a private Internet operating on GOL internal network, protected from Internet users by a firewall.

Monitoring: The analysis of content, normally with automated software, for compliance with legislation, policies and the MAC Code of Conduct. The officer designated to monitor the system can see the websites staff access, their bandwidth, and turn it off or disrupt your connection if using too much.

Personal Information: Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal use: Activity conducted for purposes other than accomplishing official business or educational and self-development purposes that are consistent with government policy. Personal use of Internet, email or other ICT facilities and devices is a privilege not a right and may be revoked at any time. Such use must be limited and reasonable, that is:

- be infrequent and brief in its usage
- be lawful, ethical and efficient in the use and management of the facilities
- must, wherever possible, take place during non-work time (e.g. during lunch breaks)
- must only incur minimal additional cost to the department.
- must not impact on the authorized user’s productivity
- must not be unauthorized as defined in this policy
- must not interfere with the operation of the agency, or related legislation and regulations
- must not embarrass or compromise the department.

Pornography: The explicit description or exhibition of sexual activity intended to stimulate erotic rather than aesthetic or emotional feelings.

Public Records: As defined by the Freedom of Information Act of 2010 (FOIA), Section 1.3.12, a “Public Record means a record, manual rule book, regulation or other documents produced or received by, being used or having been used by, possessed by or under the control of a public authority, whether in written form or recorded or stored in electronic form or in any other device.”

Security controls: Hardware, procedures, policies and physical safeguards that are put into place to assure the integrity and protection of information and the means of processing and accessing it.

Spam: The inappropriate attempt to use email, or another networked communications facility by sending the same message to numerous people who didn’t ask for it.

Streaming: Allows users to see and hear/see an audio/video file as its transferred. Streaming video is usually sent from pre-recorded video files, but they can also be broadcast live

Unauthorized use of MAC Internet, email and other ICT facilities and devices is use by any person who is not an authorized user, or any unlawful, criminal, excessive personal use or inappropriate use.

Unlawful use is use that violates any law in force in the Republic of Liberia.

User authentication: Process of validating that a user is who s/he represents her/himself to be.

Virus and malicious code: A piece of computer software or code introduced into another program for malicious purposes.

APPENDIX II: General Password Construction Guidelines

GOL staff will be required to use passwords for various purposes, including: user-level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Strong passwords have the following characteristics:

- Contain 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, !@#$%^&*()_+|~-=\ {}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

  NOTE: Do not use either of these examples as passwords!

By contrast **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:
  - Names of family members, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "GOL", "Lib", "liberia" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

APPENDIX III: Additional Guidance for Email Security and Use

In common with other channels for communication within GOL, email accounts are provided for work purposes and messages should be accurate, courteous and necessary. Messages should not be sent to a larger audience than is reasonably justifiable, particularly when they contain attachments.

Do not leave a machine which is logged into your email account unattended, unless it is disabled by a password protected screen saver and do not leave your password written on a piece of paper adjacent to your machine. Others may use it to gain access to your email and may impersonate you in sending email. Also you should not disclose the password which you use to gain access to your account to others as they may use your account to impersonate you in sending email. In either case you will be the one held responsible, until you can prove that you were not (which may be difficult).

If you receive email coming from a particular individual, but out of character with their normal style, treat it as the result of possible impersonation until you have had the chance to confirm it as genuine.

Take great care when addressing email messages, to avoid mis-delivery. You are well advised not to send, via email, material which you would not be happy sending in an unsealed envelope, unless you have made explicit arrangements to exchange the material via a secure email channel with the recipient. Ensure that email sent to you 'for your eyes only' is not sent to unattended shared printers and that printed copies of emails are not left lying around.

Be very careful when sending documents as attachments because Word and Excel files may contain information relating to earlier corrections to the document or material which previously occupied the disk space currently occupied by your file. Whilst this hidden material is generally not seen by the recipient under some circumstances it might be. Word files sent in RTF format (Save As RTF from the files dialog) greatly lessen this danger and in most cases are smaller in size. In addition they have the advantage of being readable by ALL versions of Word and many other packages.

Check all incoming attachments to ensure that they are genuine document files (.DOC, .XLS, etc.) and are not executable files (.COM, .EXE, etc.) which may carry viruses, etc., before clicking on them to open them up.

Bear in mind that legal proceedings may result from inadvertent or negligent disclosure of medical records, confidential employment records or commercially sensitive information. Considerable problems, embarrassment and expense might be caused by the inadvertent disclosure of confidential information. Email may be treated as written evidence in law. Any email which forms part of a commercial negotiation or contract for goods, services or employment might be required as evidence in a court of law and should be carefully stored in a folder where it is unlikely to be deleted accidentally.

Ensure that email is not used to defame others, as such e-mail might come back to haunt you. There have been cases where companies/institutions have been found liable for the email activities of their employees and have been forced to take severe disciplinary proceedings against offenders.

APPENDIX IV: Best Practice Procedures for Sending Business Emails

All GOL staff are required to follow the best practice procedures outlined below when using email as a way of communicating and conducting official MAC business –

- ensure a meaningful subject line is included in all email messages;
- avoid leaving blank subject lines;
- include a file reference (where possible) in the subject line or the body of the message;
- include a detailed signature and salutation block;
- ensure that the email message is captured into an approved MAC recordkeeping system once the exchange of emails between officers is complete;
- avoid sending "heat of the moment" emails;
- check the email message for accurate spelling, punctuation and grammar;
- avoid attaching/sending large documents to emails (particularly during business hours); and
- consider the option of linking to particular documents rather than including as attachments.

APPENDIX V: Versions

- 2 Dec 2015, ver. 3.4d - Final