E-Mail Policy

Ministry of Justice, R.L.

Introduction

The purpose of this E-mail Policy is to ensure that Ministry of Justice staff are fully aware of the rules governing the use of e-mail and to outline what constitutes acceptable and unacceptable use of email systems and services at the Ministry.

The Ministry of Justice (MOJ) encourages the use of electronic communications to share information and knowledge in support of the Ministry's Mission, Vision and Core Values. Electronic mail (E-Mail) is a significant electronic communication tool and staff need to be aware of their personal responsibilities with regards to its use and the potential consequences resulting from misuse.

Ministry staff who are assigned individual email accounts should use their MOJ email address to communicate in their work capacities at all times. This will promote professionalism and standardization across the Ministry, and will help ensure copies of all work correspondence are archived.

The risk that e-mails can be read by someone other than the intended recipient is real and cannot be ignored. This is particularly the case when email is sent or received from outside the Ministry email system. Emails may also be tendered in court as evidence and are subject to legal processes such as disclosure and subpoena. Staff should always consider that emails may be seen by others than the intended recipient when composing email messages.

Ministry employees should have no expectation of privacy in anything they store, send or receive on the Ministry's email system, as the Ministry may monitor messages without prior notice. However, the Ministry is not obligated to monitor email messages.

This policy is directed at and applies to all authorized users of email at the Ministry of Justice, and should be read in conjunction with the Government of Liberia ICT Handbook and related standards, codes of conduct, and laws and regulations of the Republic of Liberia.

Obtaining your email account details

All staff whose job function requires them to communicate by email will be issued with a Ministry of Justice email account. In order to receive their email account details, the member of staff is required to agree to this email policy. The ICT section will provide you with your account details, a temporary password and this policy which you are required to sign for as having received the account details and agreeing to the policy. Signing into your email account at all subsequent times is implicit agreement to the email policy, which is available on the Ministry's website or from the ICT section.

All staff must change their email password from the temporary one issued by the ICT section. This ensures the security of your email account and that only you have access to it.

E-Mail Account Security

STAFF ARE RESPONSIBLE FOR THE SECURITY OF THEIR EMAIL ACCOUNT DETAILS AND MUST NOT DIVULGE THESE DETAILS TO ANYONE ELSE.

Some basic email account security guidelines are as follows:

1. Create a password for your e-mail account to prevent unauthorized access to your e-mail. Passwords need to be such that they cannot easily be guessed. Refrain from using husband/wife/children names and significant dates like anniversaries and birthdays. It is recommended that you solicit the help of the ICT Section if you need assistance in this process.
2. If leaving your computer on and unattended for any period of time, then log out of your email account to prevent unauthorized access while you are away. As an additional security measure, you can press CTRL/ALT/DEL and select 'LOCK COMPUTER' to prevent unauthorized access to your entire computer.
3. If you suspect your account details have been compromised in any way, contact the ICT Section who will advise on action to be taken.
4. Any e-mail issues or faults should be reported to the ICT Section who will perform any necessary corrective measures.

Acceptable Use

Staff at the Ministry of Justice are encouraged to use e-mail to communicate in their work capacities. The types of activities that are encouraged include:

1. Communicating with fellow employees, business partners, clients and other stakeholders within the context of your individual assigned responsibilities.
2. Acquiring or sharing information necessary or related to the performance of your individual assigned responsibilities.
3. Participating in educational or professional development activities.

Unacceptable Use

The following activities are deemed inappropriate uses of the MOJ e-mail systemand are prohibited:

1. Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
2. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others including "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages).
3. Use of e-mail in any way that violates MOJ, MOPT or GOL policies, rules, or administrative order. For more information please see the Government of Liberia ICT Handbook issued by the MOPT at http://www.moj.gov.lr/resources/TBA.
4. Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachments) should be 10MB or less.

5. Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
6. Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
7. Excessive personal use of Ministry e-mail resources. The MOJ allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.
8. Use of the Ministry e-mail system and services for unsolicited mass mailings, commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.
9. Use of an MOJ email address when posting on social media for personal reasons.

Email Content and Security

Email is a potential route through which your computer can be affected by viruses, email bombs, Trojan horse code or other malicious code. They may not only affect your computer, but can also affect other computers on the Ministry's network. You should therefore exercise caution when opening emails and attachments, which may disguise threats such as:

- Viruses, worms and Trojan Horses, which are computer programs that can infect the computer it is on as well as all computers connected to it by a network. They are often sent as attachments disguised as useful files or programs. For example, an email containing an attachment called "MY_SCHEDULE.EXE" is probably a virus (note the .EXE at the end – this is an **exe**cutable program that will run when you open it).
- Malware, Adware, Spyware, and Ransomware are similar to viruses, but can also annoy, intimidate, spy, track, obstruct, and cause damage to the person using the computer, not just the computer itself. For example, an email containing an attachment called "FACEBOOK.EXE" is probably malware.
- Phishing, Pharming, and Spoofing, which are harmful techniques utilizing fake emails and messages that attempt to get your passwords for accessing online services or even your email account. Some may send you to a fake website created to look like the authentic one. Criminals use these fake websites to steal personal and financial information from email users. For example, an email that appears to come from a bank asking to confirm account credentials is probably fake and from someone trying to gain access to your personal financial information.

Email servers have limits on the size and type of content that can be sent. Limit the size of files sent by email to under 5MB, and periodically delete emails with large files and attachments from your mailboxes. If you need to communicate a large file, contact the ICT section who will advise the best way to do so.

Approved: _____ Date: June 14, 2016

Cllr. Wheatonia Dixon-Barnes,
Deputy Minister for Administration, Ministry of Justice, R. L.