LIBERIA MEDICINES & HEALTH PRODUCTS REGULATORY AUTHORITY

[LMHRA]

Email and Communication Policy

P.O BOX 1994
Cell: +231-777140555/888140555
Email: info@lmhra.gov.lr
Website: www.lmhra.gov.lr

Document Code: ICT-POL-002	**Date of Issue: April 13, 2026**
Version: 01	**Date of Implementation: April 16, 2026**

CONTENTS

1.0 PURPOSE....3
2.0 SCOPE....3
3.0 POLICY STATEMENT....3
4.0 GUIDING PRINCIPLES....3
5.0 DEFINITIONS....4
6.0 ACCEPTABLE USE OF EMAIL & COMMUNICATION SYSTEMS....4
6.1 PERMITTED USE....4
6.2 LIMITED PERSONAL USE....4
7.0 PROHIBITED USE....5
8.0 EMAIL SECURITY REQUIREMENTS....5
8.1 AUTHENTICATION & ACCESS....5
8.2 ENCRYPTION....5
8.3 ATTACHMENTS & LINKS....5
8.4 PHISHING PREVENTION....5
9.0 COMMUNICATION CONTENT STANDARDS....6
9.1 PROFESSIONAL TONE....6
9.2 OFFICIAL REPRESENTATION....6
9.3 CONFIDENTIALITY....6
10.0 USE OF INSTANT MESSAGING & COLLABORATION TOOLS....6
11.0 USE OF PERSONAL DEVICES (BYOD)....7
12.0 RECORDS MANAGEMENT....7
13.0 MONITORING & LOGGING....7
14.0 INCIDENT REPORTING....7
15.0 THIRD-PARTY ACCESS....7
16.0 VIOLATIONS & ENFORCEMENT....8
17. POLICY REVIEW....8
18. APPROVAL....8

1.0 PURPOSE

The purpose of this Email & Communication Policy is to ensure that all electronic communications conducted through LMHRA systems are secure, professional, lawful, and aligned with the Authority's regulatory mandate.

This policy establishes rules for the appropriate use of LMHRA email accounts, messaging platforms, communication tools, and digital correspondence to protect LMHRA's information assets and reputation.

2.0 SCOPE

This policy applies to:

- All LMHRA staff, contractors, consultants, interns, and partners
- All LMHRA-issued email accounts and communication platforms
- All devices used to access LMHRA email or communication systems
- All internal and external communications conducted on behalf of LMHRA
- All third-party service providers using LMHRA communication channels

3.0 POLICY STATEMENT

LMHRA email and communication systems must be used responsibly, securely, and professionally. All users must protect LMHRA information, comply with legal and regulatory requirements, and ensure that communications reflect the Authority's values and mandate.

4.0 GUIDING PRINCIPLES

- **Confidentiality** — Sensitive information must be protected from unauthorized disclosure.
- **Integrity** — Communications must be accurate, complete, and unaltered.
- **Professionalism** — All communications must reflect LMHRA's standards and reputation.

- **Security** — Email and communication tools must be used in a manner that minimizes cybersecurity risks.
- **Compliance** — Align with ISO 27001, Liberia Data Protection Act, and national ICT regulations.
- **Accountability** — Users are responsible for all actions performed under their accounts.

5.0 DEFINITIONS

- **Official Email Account:** An email address issued by LMHRA for business use.
- **Personal Email Account:** Any non-LMHRA email address.
- **Sensitive Information:** Confidential or Highly Confidential data as defined in LMHRA's Data Classification Policy.
- **Communication Tools:** Email, instant messaging, video conferencing, SMS, collaboration platforms, and official social media channels.

6.0 ACCEPTABLE USE OF EMAIL & COMMUNICATION SYSTEMS

6.1 PERMITTED USE

LMHRA email and communication systems may be used for:

- Official LMHRA business
- Regulatory correspondence
- Communication with stakeholders, partners, and government institutions
- Internal collaboration and information sharing
- Approved project-related communication

6.2 LIMITED PERSONAL USE

Limited personal use is permitted if:

- It does not interfere with work duties
- It does not violate LMHRA policies
- It does not consume excessive system resources
- It does not involve inappropriate or illegal content

7.0 PROHIBITED USE

Users must not use LMHRA email or communication systems to:

- Send or forward offensive, discriminatory, or inappropriate content
- Share confidential or highly confidential data without authorization
- Conduct personal business or political activities
- Send chain letters, spam, or mass unsolicited messages
- Download or open suspicious attachments
- Use personal email for official LMHRA business
- Engage in harassment, fraud, or misrepresentation
- Store or transmit pirated or illegal materials

8.0 EMAIL SECURITY REQUIREMENTS

8.1 AUTHENTICATION & ACCESS

- Strong passwords must be used.
- Multi-factor authentication (MFA) must be enabled where available.
- Email accounts must not be shared.
- Access must be revoked immediately upon staff separation.

8.2 ENCRYPTION

- Sensitive information must be encrypted when transmitted via email.
- Highly Confidential data must not be sent via email unless approved and encrypted.

8.3 ATTACHMENTS & LINKS

- Users must verify the legitimacy of attachments and links.
- Suspicious emails must be reported to the ICT Unit immediately.

8.4 PHISHING PREVENTION

- Users must not click unknown links or provide credentials via email.

- ICT Unit will conduct periodic phishing awareness exercises.

9.0 COMMUNICATION CONTENT STANDARDS

9.1 PROFESSIONAL TONE

All communications must be:

- Clear, respectful, and professional
- Free from slang, insults, or inappropriate language
- Grammatically correct and aligned with LMHRA communication standards

9.2 OFFICIAL REPRESENTATION

Users must not:

- Speak on behalf of LMHRA without authorization
- Issue public statements without approval
- Use LMHRA email for personal opinions presented as official positions

9.3 CONFIDENTIALITY

Users must ensure that:

- Sensitive information is shared only with authorized recipients
- Emails are double-checked before sending
- "Reply All" is used only when necessary

10.0 USE OF INSTANT MESSAGING & COLLABORATION TOOLS

- Only LMHRA-approved platforms may be used for official communication.
- Sensitive or Highly Confidential data must not be shared on instant messaging tools unless encrypted and approved.
- Chat histories must not be used to store long-term records.
- Users must log out of communication tools when not in use.

11.0 USE OF PERSONAL DEVICES (BYOD)

- Personal devices may access LMHRA email only if approved by ICT.
- Devices must have up-to-date security patches and antivirus software.
- Lost or stolen devices must be reported immediately.
- LMHRA reserves the right to remotely wipe LMHRA data from personal devices.

12.0 RECORDS MANAGEMENT

- Emails containing official records must be archived according to LMHRA's Records Management Policy.
- Users must not delete emails that are subject to audits, investigations, or legal holds.

13.0 MONITORING & LOGGING

- LMHRA reserves the right to monitor email and communication systems for security, compliance, and operational purposes.
- Monitoring will be conducted in accordance with national laws and LMHRA policies.
- Users will be notified of monitoring practices through this policy.

14.0 INCIDENT REPORTING

Users must immediately report:

- Suspicious emails
- Accidental disclosure of sensitive information
- Lost or stolen devices
- Unauthorized access to email accounts
- Any communication-related security incident

Reports must be submitted to the ICT Unit.

15.0 THIRD-PARTY ACCESS

- Vendors and partners must sign confidentiality agreements before accessing LMHRA communication systems.
- Access must be time-bound and monitored.

- Third parties must comply with LMHRA security requirements.

16.0 VIOLATIONS & ENFORCEMENT

Non-compliance with this policy may result in:

- Disciplinary action
- Revocation of access privileges
- Contract termination (for vendors)
- Legal action where applicable

17. POLICY REVIEW

This policy must be reviewed:

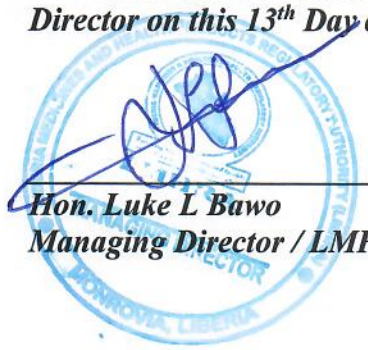
- After three years
- After major ICT incidents
- After significant organizational or technological changes

The ICT Manager is responsible for initiating the review.

18. APPROVAL

This policy becomes effective upon approval by the Managing Director of LMHRA.

The Email and Communication Policy is Hereby Promulgated and Approved by the Managing Director on this 13th Day of April A. D. 2026.



Hon. Luke L Bawo
Managing Director / LMHRA