MINISTRY OF DEFENCE AND THE REPUBLIC OF SIERRA LEONE ARMED FORCES

MEDIA POLICY GUIDELINES

Review Date: 2017 or on Demand

CONDITION FOR RELEASE

The Media Policy Guidelines contained herein is by no means a contrary tool to all existing rules and regulations, national and international; but rather should be seen as complimentary effort. The policy belongs exclusively to the Ministry of Defence (MoD) and the Republic of Sierra Leone Armed Forces (RSLAF), and by extension for the use of the wider public, upon request and so authorised by the Defence Policy Committee (DPC).

Security Classification. This document is released for the information of such persons only that need to know its contents in the course of their official duties. Therefore, any unauthorised contact with this document should be brought to the direct attention of the MINISTRY OF DEFENCE, TOWER HILL, FREETOWN, any RSLAF establishment or through the Sierra Leone Police. It should be noted that the unauthorised retention or damage of this document constitutes an offence under the Official Secrets Oath (OSO). This document is issued on an official basis and the recipient to whom it is entrusted in confidence, is solely responsible for its safe custody and ensuring that its contents are disclosed only to authorised persons.

Authentication. This document is hereby issued under the authority of Defence Policy Committee with the Minister of Defence as Chairman. More precisely, the Assistance Chief of Defence Staff for Operations and Plans is the sponsor. The Deputy Secretary for Policy and Procurement prepared the details for promulgation with the concurrence of the Chief of Defence Staff, on behalf of the Defence Council of the Republic of Sierra Leone.

Legal Status. This document has no formal status in legal terms but provides clear military guides drawn from most recent experiences and prevailing best practices, for the regulation of the affairs of MoD and RSLAF to the tune of acceptable democratic norms and values.

MR. ANDREW S. KAMARA
Deputy Secretary (Policy and Procurement)
Ministry of Defence

MAMADI M. KEITA
Brigadier General
Assistance Chief of Defence Staff
for Operations and Plans

SAMUEL O. WILLIAMS
Major General
Chief of Defence Staff
Republic of Sierra Leone Armed Forces

Authorised to sign on behalf of the Defence Council of the Republic of Sierra Leone
Dated: 20 August 2014

INTRODUCTION

1. Following a Defence Policy Committee (DPC) meeting held in the Ministry of Defence on Thursday 17 July 2014, the Media Policy Guidelines was unanimously endorsed and adopted. Advancement in media technology (new media) as an interactive form of communication that uses the internet including pod casts, really simple syndication (RSS) feeds, social networks, text messages, blogs, wikis, virtual words and other user general platforms are of importance to MoD/RSLAF personnel both professionally and personally.

2. MoD/RSLAF personnel are encouraged to talk about their roles but within the borders of privacy, security and reputation. There is an increasing significance of this mode of engagement to keep in touch with family and friends in social media which include social networking sites, blogs and other self publishing platforms on the internet. If online, MoD/RSLAF personnel must be wary about their scope of engagement as: not to breach the Official Secret Act, protect personal information, maintain operational security and be careful about the information we share online.

3. This policy is therefore, intended to guide MoD/RSLAF personnel (including civilian employees) on the scope of their online engagement within and outside the country thereby regulating cyber security and traffic.

RATIONALE

4. Media handling is now an integral part of the Armed Forces and other security agencies. We must train people for it, and commanders at all levels are expected to make good use of media opportunities in getting the right message across. All we must attempt to do is to communicate, get our stories, views and reactions across to the public through the media in an authorised, accurate, professional, timely and or favourable manner.

PROBLEM STATEMENT

5. Since the restructuring of MoD/RSLAF and the establishment of the Directorate of Defence Public Relations and Information, there has never been any Media Policy Guidelines from the Ministry of Defence that sets the objectives and standards of our personnel engagement with the Media. To date, censorship on unauthorised media engagement is only being ensured by some formations and units through SOPs which are seldom enforced.

6. As a result of this, officers and men, and civilian counterparts have been finding pleasure in directly or indirectly contacting the Media at will, thereby letting out to the public classified information without recourse to the negative impact this has on the institution. The MoD/RSLAF has faced embarrassment few times due to such practice. It is against this backdrop that this

policy guideline seeks to provide direction on our engagement with all media categories both within and outside Sierra Leone.

APPLICABILITY

7. This policy document applies to all MoD/RSLAF personnel (including civilian employees) within and outside Sierra Leone.

GENERAL GUIDELINES

8. MoD/RSLAF personnel must:

- Adhere to high standards of conduct and behaviour online as is reasonably expected.
- Protect personal information and maintain operational security, and be careful about the information you share online.
- Never speak to the Media without authority. The real challenges lie with those of appropriate authority.
- Seek authorisation from your chain of command when appropriate before speaking to the Media.
- Not post images on internet that may tarnish the image of the MoD/RSLAF.
- Protect all passwords and if necessary do not share computers.
- Be very careful on what you place on Social Media.
- Not attempt to gain unauthorized access to MoD/RSLAF IT and telecoms or content for which you do not have permission (i.e Hacking).
- If you are serving with the MoD/RSLAF and at the same time operating with Blog Group(s), leader(s) of such groups must take responsibility for whatever is posted in their Blog Group(s) on social media.

CODE OF COMMUNICATION WITH THE PRESS

9. **DOs.** When engaging the **media**:

- Answer questions about your own work.
- Be positive about your own role.

- Speak with respect and sympathy about other people.
- Don't forget, you are representing your Institution.
- Remember the Name and Organisation of the Reporter.
- Report whom you spoke to and what was said.
- Refer to your superior if you don't know the answer.
- Be Brief and Precise.
- Stick to the Facts.
- Be Polite.
- All Officers should know the basic points on Defence Missions and Tasks.
- These points should be provided by your Public Relations & Information office.

10. **DONTs.** When engaging the media **don't**:

- Talk unnecessarily.
- Address questions you are not authorised to answer but refer these questions to your commander or spokesperson.
- Give personal opinion about any situation on critical issues.
- Speak about something that you don't know or is not your responsibility.
- Answer speculative questions. For example, **"what will happen if….?"**
- Disclose operational security plans or procedures.
- Discuss other Forces.
- Post your own images/pictures on social media with any kind of military uniform.
- Appear to favour one side over the other (impartial).
- Attempt to access, amend, damage, delete or disseminate another user's files, emails, communications or data without the appropriate authority.

WHO ARE AUTHORISED TO ENGAGE THE MEDIA AT FORMATIONS AND UNITS

11. The handling of the media at formation and unit levels is a command responsibility. Only the commander or his designated competent media officer is allowed to deal with the media at formation and unit levels. However, such engagement with the media should be mostly restricted to issues relating to his/her formation or unit. Complex or delicate matters on the MoD/RSLAF must be referred up the chain of command or to the Directorate of Defence Public Relations and Information.

CATEGORIES OF DOCUMENTS TO BE RESTRICTED TO THE PRESS

12. All intelligence, security and key operations related documents **must not** be disclosed to the Media without the appropriate authority. These restricted documents may be in the form of video clips, photos, tapes, electronics or hard copies.

USE OF INTERNET

13. In a number of instances, MoD/RSLAF personnel have posted comments, queries and concerns on social media sites provoking unwarranted media spotlight and heightening public concerns. The under-mentioned guidelines are therefore intended to strategically regulate the MoD/RSLAF cyber traffic for service personnel (including civilian employees) making personal use of the internet and they apply to any engagement with the website, blog photo or video channel, bulletin board or online forum, social net work or multi player game.

14. **In summary, you must not knowingly transmit:**

- Offensive, indecent or obscene material or abusive images and literature.

- Materials which can be reasonably considered as harassment or insulting to other people or organisations.

- Materials obtained in violation of copyright or used in breach of a licensed agreement.

- Spam (electronic junk mail) or chain email.

- Materials that could by their presence on the MoD/RSLAF website reasonably are expected to embarrass or compromise the chain (although reasonable comments that disagree with the MoD/RSLAF are allowed).

- Commercial activities connected to MoD/RSLAF business.

- Any form of gaming, lottery or betting.

- Any form of share dealing.

- Materials designed to mislead people about who originated or authorised it (eg. through misuse of signatures).

- Attempt to compromise MoD/RSLAF IT and telecoms, prevent legitimate access, damage or seek to cause degradation of performance or a denial of service.

- Attempt to gain unauthorised access to MoD/RSLAF IT and telecoms or contents for which you do not have permission (i.e. hacking).

15. **MoD/RSLAF personnel making personal use of the internet:**

- Are expected to adhere to the same high standards of conduct and behaviour online as they would in any other aspect of their professional or personal lives.

- Should beware of the dangers to themselves and others in sharing information online.

- Are allowed to identify themselves as MoD/RSLAF personnel for example in a user profile or photograph.

- Should not publish info about third parties (including colleagues) without their permission.

- Do not need to seek clearance to publish material not connected with work. For example; material relating to personal interest and hobbies.

- Must seek authorisation before publishing any wider information relating to work which:
  - Reflects on wider Defence and Armed Forces activity.
  - Attempt to speak or could be interpreted as speaking on behalf of the MoD/RSLAF.
  - Relates to classified, operational, controversial or political matters.

- Should consider using or referring to material on MoD/RSLAF corporate websites in your conversations.

- Should think about personal reputation and don't publish anything that shouldn't be seen by your family members as inappropriate.

- Are not prohibited from expressing views but should avoid being drawn into making comments on controversial matters. (E.g. on a political campaign or petition).

- Should not use rank or position when engaged on the internet (ie use Kamara not Maj Kamara or indicate you are MoD Civil Servant as this could be taken as official document).

- You are not prohibited from editing wikis if you have useful information to contribute.

- Can act anonymously or pseudonymously in a personal capacity where appropriate but must:

    - Still follow this guidance.

    - Beware that very few things on the internet are genuinely anonymous and most can be traced.

    - Understand that services, MoD/RSLAF and other authorities will pursue serious breaches of the rules, regardless of whether the person intends to publish anonymously.

- If you are unsure, always seek advice from your superior commander or your line manager before going ahead.

MANAGEMENT OF PERSONAL INFORMATION

16. Threat to your Information. Below are the main categories of information that could be at risk, for the hostile groups that might seek this information and the potential consequences if the information is compromised:

a. Personal Information. Personal information is always at a premium in the criminal and espionage world. Items of information which can be used to take advantage of you and your family can include:

- Full Name
- Date and Place of Birth
- Full Home Address
- Telephone Numbers
- NASSIT Numbers
- Passport Details

17. Information such as this may give away personal details about yourself unintentionally through the linkages you make with other people. For example, by looking at your friends information on a social net working site it would be fairly easy for a stranger to work out roughly where you live and your approximate age, even if you have not volunteered any of these information yourself. This makes it even more important to safeguard the exact details of your personal information describe above:

b. Account Details. Criminal groups may also try to gain access online, telephone or other accounts using your details. This includes information such as:

- Account Numbers.
- Login or User IDs.
- Password.
- Pin Code Numbers.
- Memorable Phrases.
- Security Questions.

18. Information such as these could be used for criminal activity or blackmail. Do not give this information to third parties:

c. Details About Your Work. Hostile intelligence services or terrorist organisations may seek details about your work or your establishment/unit. This may include:

- Establishment/Unit Location.
- Work Telephone Number.

- Rank/Staff/Service Number.
- Position/Role.

19. Information such as these could enable your establishment/unit to be targeted. Protect this information and specifically, do not disclose:

- Any protectively marked Information.
- Any connection with or mention of Operation.

20. Images can give away important information unintentionally. Check to make sure Forces ID, sensitive materials or equipment is not visible.

Operational Information. If you are involved in an operation directly or supporting it, information protection becomes even more important and attempts to gather information by hostile agencies or groups may become more determined. Information that will be of interest to these groups includes:

- Operational Programmes.
- Deployment Details.
- Capability Shortfalls.
- Casualty Details.
- Morale.
- Mission-Specific Information.

21. Information such as this can be used by an enemy in countering our operations, putting lives and assets at greater risk. It may also damage our credibility with our allies and possibly lead to a withdrawal of their support. Do not release on line.

PROCTECTING YOUR INFORMATION

22. As well as withholding the types of information described above, there are a number of simple steps you can use to protect yourself online.

- Underline and apply your security settings.
- Choose your online friends carefully and be circumspect with the information you share

with them.

- Only post items that would be acceptable to your family, friends or colleagues.

- Make sure photographs don't give away information you want to protect.

- Do not give out unnecessary information when registering.

To maintain security on the Web the following are general good practice:

- Do not share your loggings or password.

- Change password regularly.

- Use a password that would be difficult to guess. Don't use simple words and mix upper and lower case-characters and materials.

PROTECTING FRIENDS' AND COLLEAGUES' INFORMATION

23. Some social networking sites enable you to publish information about other people, for example by identifying them to photographs. Be careful about disclosing information about friend and colleagues. Respect their privacy and maintain their security:

- Breaching of rules or the handling of other peoples' personal information is potentially a disciplinary offence.

- Take care not to disclose personal information about your friends and colleagues that they might want to keep private. For example medical or family problems or forthcoming deployments.

- Be wary of publishing group or course photos which link individuals to organisations. Are all the people in your photographs happy to be identified?

- Exercise particular care in posting photographs or other information about third parties working with the MoD/RSLAF. You could inadvertently place them at risk.

PENALTIES

24. It shall constitute an offence under the RSLAF Act 1961 as amended, the Official Secret Act and any other Statutory Instruments by knowingly and or unknowingly compromising the operational security which may infringe on national security and the personal security of others.

POLICY REVIEW

25. With the passage of time and emerging trends in information processes, procedures and daily engagement, these policy guidelines are therefore subject to review.

CONCLUSION

26. As interactive form of communication necessitates the use of the internet including social network, it must be borne in mind that, security is everybody's responsibility. Our own personnel are our eyes and ears on the internet. If you see any information that falls into one of the categories under information protection, that you suspect may have been released without proper authorisation, contact your appropriate superior authority immediately so that mitigating action can be taken. Neither Commanders nor staff should attempt to remove third party material from the internet without authorisation and advice from relevant/appropriate authorities.