

RESTRICTED

The information contained in this handbook is not to be communicated either directly or indirectly to the press or to any person not authorised to receive it



DEFENCE HEADQUARTERS

**POLICY ON THE USE OF
SOCIAL MEDIA FOR THE
ARMED FORCES OF NIGERIA**

Prepared under the direction of:

Abuja
11 June 2018

A red ink signature, appearing to read 'AG Olonisakin Nam', is written over a horizontal red line.

AG OLONISAKIN NAM
General
Chief of Defence Staff

i
RESTRICTED

CONDITION FOR RELEASE

The intellectual property rights for this publication belong exclusively to Defence Headquarters. No material or information contained in this publication should be reproduced, stored in a retrieval system or transmitted in any form outside the Ministry of Defence establishments except as authorized by both Defence Headquarters and the Ministry of Defence where appropriate.

This information may be released by the Government of the Federal Republic of Nigeria to a recipient Government for defence purposes only. It may be disclosed only within the Defence Department of the recipient Government, except as otherwise authorized by the Ministry of Defence.

Comments on factual accuracy or proposals for amendment should be directed to:

The Chief of Defence Standards and Evaluation
Department of Defence Standards and Evaluation
Defence Headquarters
Area 7 Garki
Abuja

Abuja
11 June 2018



LKJ OGUNWE
Maj Gen
CDSE

FOREWORD

1. The use of social media is on the increase globally. Social Media is also used by members of the Armed Forces of Nigeria (AFN) and its impact to personnel on operational and national security cannot be over emphasized. Therefore, managing and regulating the use of Social Media by members of the AFN is critical to the daily, operational and strategic needs of the AFN.

2. In line with my vision for the AFN which is to "*ensure a well-motivated, trained and equipped Armed Forces that is responsive to national security commitments*", I directed that the existing policy on the use of Social Media for the AFN be revised in accordance with modern dictates, and the increase use of Social Media by members of the AFN, which has great impact in our dynamic operational environment.

3. The Defence Space Administration (DSA) is the lead agency for the overall implementation and monitoring of the **Policy on the Use of Social Media for the AFN**. The coordination, control and supervision of the use of Social Media by personnel of the AFN is also the responsibility of DSA. I therefore commend the CDSA and the personnel who helped in making the current **Policy on the Use of Social Media for the AFN** a reality. I strongly commend that all Service personnel should get acquainted with the policy as it relates to their activities in the AFN.

Abuja

11 June 2018



AG OLONISAKIN NAM
General
Chief of Defence Staff

PREFACE

1. Social Media is a platform containing a collection of applications and software that allows users to create a profile, upload photos and videos, send messages, and share information over the internet. These platforms are readily available, user friendly and easily accessible. They are very effective tools in information sharing and Media Operations that are utilized by both friendly and enemy forces. Military establishments use social media mainly to support military operations such as PsyOps, OSINT, Counter Narratives, Cyber espionage and for offensive purposes including propaganda. The potentialities of these platforms are enormous and their control, monitoring and use are very critical particularly as it relates to military operations and national security.

2. To avoid compromising OPSEC by misrepresenting the AFN or divulging vital information, it is incumbent for the AFN to streamline how members of the AFN use Social Media platforms both for official and personal purposes. The Policy on the Use of Social Media by members of the AFN would therefore ensure that they present themselves in a professional and responsible manner on Social Media platforms. OPSEC and personal privacy concerns should be considered when using Social Media bearing in mind the codes and ethics of the AFN as well as the Official Secrets Act as guiding rules.

3. In line with its mandate, DSA would closely monitor, supervise and control the use of Social Media by members of the AFN. Personnel found to have defaulted in the provisions of this policy would be adequately sanctioned to ensure that good order and discipline is maintained in the use of Social Media.

Abuja

11 June 2018



EG WHYTE

Maj Gen
CDSA

TABLE OF CONTENTS

Serial	Title	Pages
(a)	(b)	(c)
1	Title Page	i
2	Record of Amendments	ii
3	Condition for Release	iii
4	Foreword	iv
5	Preface	v
6	Table of contents	vi
7	List of Abbreviations	vii
8	Introduction	1
9	Classification of Social Media Platforms	2
10	Responsibility of Monitoring the Social Media for the AFN	3
11	General Guidelines on the Use of Social Media for Personnel of the AFN	5
12	Guidelines for Official Communication with the Public on Social Media	5
13	Guidelines for Personal Use of Social Media	7
14	Security Measures to be Adopted when Using Social Media	9
15	Do's and Don'ts for Social Media Administrators for the AFN	10
16	Actions on Social Media Considered as Offences by this Policy	12
17	Conclusion	13

ABBREVIATIONS

AFN	-	Armed Forces of Nigeria
ASA	-	Appropriate Superior Authority
BRB	-	Be Right Back
GPS	-	Global Positioning System
KIA	-	Killed in Action
LMAO	-	Laughing My Ass Out
LOL	-	Laugh Out Loud
LWKMD	-	Laugh Wan Kill Me Die
MIA	-	Missing in Action
OMG	-	Oh My God
OPSEC	-	Operational Security
OSINT	-	Open Source Intelligence
PsyOps	-	Psychological Operations
WIA	-	Wounded in Action

POLICY ON THE USE OF SOCIAL MEDIA FOR THE ARMED FORCES OF NIGERIA 2018

INTRODUCTION

1. The use of software, mobile telephony and the Internet has facilitated rapid advancement in the field of communications technology. The unimaginable reach of the social media coupled with its ability to disseminate information in real time across the globe is indeed amazing. Social media has become a major part of our daily lives. It helps organizations and individuals share information and keeps personnel, family and friends connected in real-time.
2. For the purpose of this policy document, Social Media is defined as a platform where user generated content is shared over the internet using a technology that promotes engagement, sharing and collaboration. The potentialities of these platforms are enormous and their control, monitoring and use are very critical. Military establishments are mainly attracted by social media due to the possibility of being able to support military operations such as: Psychological Operations (PsyOps), Open Source Intelligence (OSINT), Counter Narratives, Cyber espionage and for Offensive purposes including propaganda.
3. There is no gainsaying that Nigeria's adversaries would be very much interested in the social media communications of the members of the Armed Forces of Nigeria (AFN) in search of information that could be of immediate or future operational value. Thus, it should be expected that adversaries constantly look for posts by AFN personnel on Facebook, Twitter, Instagram etc, and even check the GPS tags of some transmissions. In addition to deriving maximum benefits from the use of social media, the AFN needs to take measures necessary to prevent adversaries from obtaining information of operational security value from the social media communication of personnel.

4. The purpose of this policy is to set guidelines for the use of social media by members of the AFN. Although members of the AFN have the right to free speech, social media communication can have significant impact on institutional reputation and operations due to its wide reach hence the need for caution. The policy is applicable to members of the AFN and civilians working in military establishments. The policy covers social media classification, the responsibilities of monitoring the social media as well as security measures to be adopted on using social media. It also highlights the general guidelines on the use of social media, guidelines for official communication with the public, guidelines for personal use of social media, Do's and Don'ts for handlers of social media for the AFN and sanctions for the violation of the AFN Social Media Policy.

CLASSIFICATION OF SOCIAL MEDIA PLATFORMS

5. Social media can be classified into the following:

a. **Social Networking**. Social networking is the process of using websites and applications to communicate informally with others, find people and share similar interests. It allows users to directly connect with one another through groups, networks, and location. Examples include Facebook, Whatsapp, Instagram, Twitter, Snap Chat, Telegram and LinkedIn.

b. **Micro blogging**. Micro blogging is the process of posting very short entries or updates on a social networking site. It allows users to subscribe to other users' content, send messages, and reply publicly. It also allows users to create and share hashtags in order to disseminate content about related subjects. Examples include Twitter, Instagram and Tumblr.

- c. **Blogging.** Blogging refers to the recording of opinions, stories and links from other websites on a personal website. Examples include Wordpress and Blogger.
- d. **Photo Sharing.** Photo Sharing refers to the publishing of a user's digital photos, enabling the user to share with others either publicly or privately. Examples include Instagram, Flickr, Snapchat and Pintrest.
- e. **Video Sharing.** Video sharing refers to the publishing of a user's digital videos, enabling the user to share videos with others either publicly or privately. It also allows users to embed media in a blog or Facebook post, or link media to a tweet. Examples include Youtube, Vimeo, Snapchat, Instagram Stories, Periscope and Facebook stories.

RESPONSIBILITY OF MONITORING THE SOCIAL MEDIA FOR THE AFN

- 6. The duty of Monitoring the Social Media for the AFN lies with DSA and it shall have the following responsibilities:
 - a. Scour blogs, forums, chat rooms and personal websites to piece together information of interest to the AFN.
 - b. Monitor Social Media presence of personnel and ensure that sensitive and classified information are not posted to the public.
 - c. Produce training materials and conduct regular Social Media OPSEC training for members of the AFN.

d. Extend training on proper use of the Social Media to the families of personnel, as it is important to keep them just as informed and up to date as the personnel.

7. DSA has the mandate to block or delete posts of members of the AFN containing:

- a. Offensive or threatening language.
- b. Potentially defamatory or slanderous accusations.
- c. Words or sentences in Languages other than English.
- d. Spamming or Phishing.
- e. Overtly political statements.
- f. Any form of gaming, lottery or betting.
- g. Any unlawful use of imagery that violates copyright or breach of license agreement.
- h. Any use of images that may be considered abusive, offensive, indecent or obscene.
- I. Links to sites that may be obscene, offensive or indecent.

8. DSA is to set up a dedicated Facebook Group Account for members of the AFN and all personnel would be requested to join the platform.

GENERAL GUIDELINES ON THE USE OF SOCIAL MEDIA BY PERSONNEL OF THE AFN

9. The following should be considered before using any type of social media:
- a. Think it through: Ensure that you understand the context and the extent of the network before joining in terms of who the potential audience are and determine if there is a good reason for you to place a comment or response.
 - b. Be honest, cordial and professional at all times.
 - c. Do not post classified documents.
 - d. Personal privacy concerns should be paramount when using social media.

GUIDELINES FOR OFFICIAL COMMUNICATION WITH THE PUBLIC ON SOCIAL MEDIA

10. The following are guides for official representation of the AFN on Social Media:
- a. The Services are to appoint Social Media Administrators and Content Managers to be responsible for posting content online to the general public.
 - b. There shall be mandatory OPSEC training for officials who are to interact with the public on social media.
 - c. The protocols that apply when acting as an official representative of the AFN should be the same both for physical and electronic communication.

- d. Members of the AFN making comments or contributions on behalf of the AFN should only do so with necessary approval.
- e. Before engaging with a specific social media channel ensure you understand its terms of reference, convention and etiquettes.
- f. Social Media Administrators should not engage in online communication activities, which could bring AFN into disrepute.
- g. Personal details of other members of the AFN should not be given out; only the official contact details such as official cell-phone number, office telephone, e-mail for reference purposes.
- h. An official shall not post any material that is protected by copyright.
- i. When posting text and/or images, the corporate identity of the AFN and Services as a whole must be respected.
- j. In official social media online postings, reasonable efforts must be made to publish facts and statements that can be verified and not personal opinions or speculations.
- k. Any incorrect information relating to the AFN policy and operations should be identified and corrected.
- l. Refer your audience to the websites of the AFN or Services for more details where necessary.

m. Where users ask questions about policy or published information, ensure that any comment or response you make is appropriate to your role.

n. Only authorized spokespersons or duly delegated officials may provide comment to the media on AFN related issues.

o. Media enquiries about social media posts by personnel of AFN must be referred to the designated Service's Social Media Administrator.

p. Social Media should not be a platform for reporting casualties of personnel especially KIA and MIA. Similarly, medical information about personnel should not be posted on social media.

q. It is very necessary for the officials handling social media platforms to engage the public in real time. An inactive social media platform is ineffective because visitors will lose interest and stop accessing the pages. Social Media platforms are designed to support various forms of content. The officials handling the pages should take advantage of this by posting stories, videos and photos related to service missions to keep the viewers busy.

GUIDELINES FOR PERSONAL USE OF SOCIAL MEDIA

11. Service personnel are to keep in mind that there is no difference in their personality whether they make physical or electronic communication appearance. Hence, the same codes, ethics and Official Secrets Act apply in both cases and should be considered as the guiding rule. The following are further guides:

- a. Officers and men should always note that their position as members of the AFN may be known to their audience and what they say or do in their personal capacity may be misunderstood or misrepresented as an official position.
- b. Personnel should understand the privacy and security settings of the medium.
- c. Personnel are not to post sensitive information about themselves, colleagues or units such as schedules and events, locations, weapons and equipment.
- d. Personnel on operations are to turn off GPS/Location functions of phones to avoid geo-tagging.
- e. Personnel should post any video/audio recording and pictures during exercises/operations.
- f. Personnel will be held liable for any security issues arising from postings in respect of them by civilian friends or relations. They are therefore, to educate their friends and relations as necessary regarding military security and what should not be posted on social media.
- g. Personnel should not post their pictures or those of their colleagues in military uniforms, or pictures containing military structures, platforms and other military related items.
- h. Personnel who engage in personal or professional social media are not to reference the AFN on any matter.

- i. Personnel are not to use their rank, appointment or responsibilities in order to promote themselves online for personal or financial gain.

SECURITY MEASURES TO BE ADOPTED WHEN USING SOCIAL MEDIA

12. Some additional security measures to be adopted when using social media include:

- a. Never accept a friend request from someone you do not know even if they know a friend of yours.
- b. Do not share any information that you do not want to become public.
- c. Be cautious when listing your job, education as well as contact information as providing too much information can leave you exposed to people who want to steal your identity or sensitive operational information.
- d. Always adjust the privacy settings of your social media accounts to restrict sensitive information to the general public. Set your security options to allow visibility to “friends only”.
- e. Avoid using location-based social networking services to avoid geo tagging. Some smart phones and digital cameras automatically embed geotags unto pictures so always be wary of this feature by ensuring to turn off location services on such devices.

f. Imposter accounts are violations of the terms of use agreement. Most social media platforms have a reporting system that allows users to report an individual who is pretending to be someone else. Report any impersonation to the social media platform by contacting the platform directly. In case of any impersonation of a senior military officer or personnel, contact DSA for further action.

DO'S AND DON'TS FOR SOCIAL MEDIA ADMINISTRATORS FOR THE AFN

13. The DO's and DON'TS by Social Media Administrators/Content Managers are outlined below. They are however not exhaustive.

DO'S

14. DSA and Social Media Administrators in the Services are advised to carry out the following:

- a. Turn off GPS/Location functions of phones to avoid geo-tagging.
- b. Adjust the privacy settings of your social media accounts to restrict sensitive information to the general public.
- c. Always post comment in a friendly but professional manner.
- d. Spell check every post prior to posting.
- e. Have someone else read your posts before you upload them.
- f. 'Like' Sister or similar organisations and tag them often.
- g. Be mindful of Identity Theft when posting.
- h. Identify/find subject matter experts to answer questions that people ask on your page.
- i. Present logical and factual narratives after approval from ASA.

- j. Trawl the internet for information concerning the AFN real-time using predefined Social Media engagement tools and applications.
- k. Report infractions by members of the AFN to appropriate directorates for further action.
- l. Promote the strides and achievements of the AFN online without exaggeration.
- m. Post comments systematically and effectively through popular blogs, channels and platforms.
- n. Liaise with social media influencers to help promote AFN narratives.

DON'TS

- 15. The following are forbidden practices on Social Media:
 - a. Posting classified documents.
 - b. Posting any material that is protected by copyright.
 - c. Posting information on specific unit/formation movement.
 - d. Posting unsubstantiated comments and articles.
 - e. Posting political matters.
 - f. Using geo-tagged programmes.
 - g. Posting any video, audio, materials pictures during exercises/operations.
 - h. Using pseudonyms, trolls and pseudo social media accounts on AFN platforms.
 - i. Accepting a friend request from someone you do not know even if they know a friend of yours.

- j. Sharing any information that you do not want to be viral
- k. Using automated posting services to post same content to multiple sites.
- l. Posting comments and articles too many times a day.
- m. Cluttering all your posts at one time or seem to be spammy.
- n. Using social media languages such as “LWKMD, LMAO, LOL, OMG, BRB” etc in professional posts.

ACTIONS ON SOCIAL MEDIA CONSIDERED AS OFFENCES BY THIS POLICY

16. This policy considers the following actions as offensive:
- a. Unauthorized disclosure of operational information through social media.
 - b. Breach of protocol applicable when acting as a representative of the AFN.
 - c. Making comments on the AFN or members of the AFN without necessary approval from ASA.
 - d. Unauthorized disclosure of official security information through social media.
 - e. Posting videos and pictures in which personnel are found in compromising positions

f. Posting operational pictures thereby compromising troops' locations to the adversary.

g. Posting pictures of personnel KIA/WIA/MIA.

h. Flouting rules and regulations guiding marriages by posting compromising pictures and videos taken in uniform before, during and after the wedding ceremonies.

I. Being friends with social media accounts linked with disgruntled elements of the state, terrorist organizations, terrorist sympathizers, criminals and advance fee fraudsters.

17. The above stated actions are liable to prosecution and punishments as contained in the Armed Forces Act CAP A20 LFN and the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

CONCLUSION

18. The AFN is leveraging on social media to improve communication with the general public. However, there is need to exercise caution on the use of social media for communication with the public in order to ensure that operational security is not compromised. This Social Media Policy is an important first step for the safe and effective use of the social media platform by personnel of the AFN.