Defence Forces Social Media Policy

Contents

Introduction 2
Aim 2
Personal Social Media Use By Members Of The Defence Forces 3
Official Defence Forces Social Media Sites 7
Actions On Being Hacked Or Suspicion Of Being Hacked 9
Disciplinary Action 9
Annex A 11
Introduction

1. The proliferation of social media sites such as Facebook, Twitter, YouTube, Instagram, LinkedIn and others has resulted in them becoming an integral part of everyday communications for the majority of the Irish population, including members of the Defence Forces. Social media is also defined as any of the messaging services available such as WhatsApp, Facebook Messenger, Viber, etc. When utilised correctly, social media can be a powerful communications tool and can be used in both a personal and professional communications capacity.

2. When utilising social media, the lines between public and private, personal and professional are blurred. By simply being identifiable as a member of the Defence Forces, perceptions can be created about your expertise and authority to speak on behalf of the Defence Forces.

Aim

The aim of this document is:

1. To enable Defence Forces personnel to make full use of online platforms while protecting their own safety and security, as well as that of their colleagues.

2. In line with the Defence Forces communication and engagement guidelines, to harness social media in order to:
   a. Invigorate the internal audience
   b. Create advocates for the Defence Forces both internally and externally
   c. Enhance public perception

3. To outline the procedures for establishing and maintaining social media sites and to establish a code of conduct for communicating across all platforms on social media.

4. To provide guidance on how to ensure our members maintain an Accurate, Appropriate and Apolitical presence on social media.

5. To describe expected behaviour on social media, and specify conduct which would contravene GRO 43/55, Para 27 of Defence Forces Regulation A.7 Discipline, the General Data Protection Regulation (GDPR) (EU) 2016/679 and The Data Protection Act 2018.
Personal Social Media Use By Members Of The Defence Forces

1. If a member of the Defence Forces operates a social media account(s) or has any online presence, they are subject to compliance with this document when commenting, posting, tweeting, blogging, messaging, sharing, etc. any material that directly mentions or relates to the Defence Forces.

2. When commenting, posting, tweeting, blogging, messaging, sharing, etc. personnel should ask themselves:
   
a. What if this were to be published in a newspaper or magazine?

b. Would I say this to a superior, to a journalist, on the radio etc?

c. What could a malicious party do with this information?

Note that anything which is said online is potentially retrievable by Military Police and other official agencies as part of an investigation.

3. Personnel who utilise social media are encouraged to:

a. Follow the same high standards of conduct and behaviour online as would be expected in any forum.

b. Always maintain personal and operational security and be careful about the information that is shared online. If in doubt, leave it out.

c. Make family and friends aware of the operational security issues surrounding their interaction with you, or about you, online.

d. Clarify with your chain of command if at all unsure whether or not content is appropriate.

e. Provide your Brigade/Formation Press Officer with any interesting content you may have acquired relating to Defence Forces activities.

f. Share, repost, retweet, link and promote Defence Forces social media content. Below are examples from two of the platforms operated by the Defence Forces:

g. Encourage family and friends outside of the Defence Forces to join and engage with Óglaigh na hÉireann social media sites in a positive manner.
h. Report any Defence Forces account that has been inactive or has not posted in thirty (30) days to the DF Public Relations Branch. Accounts that are inactive for over thirty (30) days are deemed to be dormant, and will be deleted.

4. Personnel are prohibited from the following:

a. Publishing/posting any information that relates to operations, deployments or service within the Defence Forces without prior approval from your chain of command. Examples of this information includes, but is NOT limited to:
   (1) Security duties i.e. Portlaoise, barrack, government buildings, etc;
   (2) Armed escorts i.e. Prisoner escorts, EOD, range convoys, etc;
   (3) Armed training exercises i.e. LFTT, weapons handling, etc;
   (4) Patrols – Bde Stand To, Naval Service fisheries, Air Corps maritime, etc;
   (5) Overseas – Leave and resupply convoys, camp duties, etc.
b. Do not offer negative opinion or comment negatively on wider Defence Forces activity or related issues by posting, tweeting, blogging, messaging, sharing, etc.

c. Do not enable geo-tagging and location services on your smart devices whilst engaged on any duties or operations.

d. Do not post material that is unlawful, obscene, defamatory, threatening, harassing, abusive, slanderous, hateful, or embarrassing to any other person or entity.

e. Do not attempt to speak, or be interpreted as speaking, on behalf of the Defence Forces.
f. Do not comment on any issue relating to controversial, sensitive or political matters which would be incompatible with service in the Defence Forces. The example below was shared by a serving member who commented negatively on the PSNI (redacted)

![Image of a social media post with a red circle over it, indicating it is not acceptable content.]

Do not comment on any issue relating to controversial, sensitive or political matters which would be incompatible with service in the Defence Forces. The example below was shared by a serving member who commented negatively on the PSNI (redacted).

![Example social media post showing alcohol with weapons, smoking indoors, drinking in uniform, etc.]

Do not create any social content that could cause the Defence Forces to be embarrassed or brought into disrepute. The below example shows alcohol with weapons, smoking indoors, drinking in uniform, etc.

![Example social media post with comments from other users indicating it is not appropriate content.]

Do not forward screenshots or share photos/material via sites or messaging services by other people that contravene this policy.

i. All comments, posts, tweets, blogs, messages, shares, etc. should be Accurate, Appropriate and Apolitical.

h. Do not forward screenshots or share photos/material via sites or messaging services by other people that contravene this policy.
Defence Forces Social Media Policy

Official Defence Forces Social Media Sites

1. Defence Forces Public Relations Branch has the sole authority to establish and operate social media platforms on behalf of the Defence Forces on any social media site which is assessed as of benefit the organisation within Defence Forces communication guidelines.

2. All official Defence Forces Social Media platforms must utilise two-step authentication procedures where available to enhance security. They should also enable e-mail notifications of unrecognised logins.

3. Establishment of social media platforms at any other level of the organisation is at the discretion of OIC Public Relations Branch. Before applying to set up an account, the following considerations should be made:
   a. Does the capacity exist to produce a minimum of two engaging and well composed posts per week?
   b. Are there alternate personnel available and capable of maintaining the account to the same high standard in the main account holder’s absence?
   c. Is the content better served on this new account, rather than being propagated on the main DF accounts?
   d. If the answer to any of the previous questions is ‘No’, the minimum criteria for establishing an account has not been met.

4. Brigade and formation social media platforms
   a. The only sanctioned social media platform to represent Brigade and Formation level is Facebook. This is because Facebook as a platform allows for more detail to accompany content in publicising the Defence Forces than other platforms.
   b. Social media platforms may only be operated if there is a designated PIO responsible for the account at all times.
   c. If a brigade or formation wishes to utilise any additional social media platform, permission must be approved by GOC/Fmn Commander and notified to OiC Public Relations Branch. Before setting up an account, considerations as per Official Defence Forces Social Media Sites, para 3.a to 3.d should be applied.
   d. Brigade/Formation Press Officers should be proactive in providing suitable content to both the DF Public Relations Branch and their own platforms across a broad spectrum of media in order to ensure optimum representation of their respective brigades or formations on the various Defence Forces platforms.
e. Brigade and formation social media platforms will be used to primarily share content from the main Defence Forces platforms as well as:

(1) Invigorating the internal audience with content unique to the formations capabilities, events or achievements by personnel and provide an outlet for its subordinate units, clubs, societies etc;
(2) Interacting with followers to create advocates both internally and externally;
(3) Sharing previously published content from other Defence Forces platforms in order to enhance the perception of the Defence Forces.

f. Brigade and formation social media platforms will NOT:

(1) Publish anything of an operational nature which could compromise the security of Defence Forces personnel or associated groups;
(2) Upload video or imagery that reflects poorly on the Defence Forces, or display security sensitive information;
(3) Allow social media platforms to replace or encroach on the importance of routine orders, talks to troops, noticeboards, etc. as the primary means of communicating information.

5. Unit, sub-unit and school social media platforms

a. Units and sub-units

(1) Units are NOT permitted to operate their own social media platforms without approval of Bde/Fmn Commander and notification to OiC PR Branch;
(2) Unit commanders may utilise ‘Twitter’ to engage locally as representatives of their unit;
(3) This account should be a titled as opposed to a personal name i.e. ‘Officer Commanding 21 Infantry Battalion’;
(4) If Unit commanders wish to include personal information such as their name or alternate contact details in the description area of the platform, they may do so.
(5) This should also be a legacy account that is passed by the outgoing OC to the incoming OC in order to maintain the links established to local social media accounts.
(6) Before setting up an account, considerations as per Official Defence Forces Social Media Sites, para 3.a to 3.d should be applied.

6. Groups, clubs and associations within the Defence Forces

a. Groups, clubs and associations are NOT permitted to operate their own social media platform(s), but are allowed to make a case if there is a requirement for them to do so.

b. Please note all applications will be assessed on a case by case basis and are at the discretion of OIC Public Relations Branch. Before applying to set up an account,
considerations as per Official Defence Forces Social Media Sites, para 3.a to 3.d should be applied.

7. The General Data Protection Regulation (GDPR) (EU) 2016/679 and The Data Protection Act 2018 are applicable to the processing of personal data, which includes social media. Operators of sanctioned Defence Forces social media accounts should consult the Defence Forces Administration Instruction A.8, in particular Chapter 4 - Defence Forces Data Protection Policy to ensure compliance. Please see Annex ‘A’ for a flowchart guide for utilising content on Defence Forces social media accounts.

**Actions On Being Hacked Or Suspicion Of Being Hacked**

1. Please note: all of these actions should be completed IMMEDIATELY on discovery of an official Defence Forces social media account being hacked.
   
   a. Immediately log the affected/suspected account out of all devices. All social media platforms have this option within their settings.
   
   b. Log back in and change the password of the affected/suspected platform to a completely different password. (Utilise letters, numbers and symbols in the new password)
   
   c. If unable to log back in, notify the platform company through its helpdesk and follow the procedures laid out by the developer, as this varies between platforms.
   
   d. Notify Public Relations Branch through the chain of command.

**Disciplinary Action**

1. Should personnel have any online interaction which represents themselves, and by extension the Defence Forces in a negative light as outlined previously, they should be aware of the following:
   
   a. Failing to comply with this instruction will result in disciplinary action and they will be obliged to remove any social content as directed.
   
   b. Section 169 of the Defence Act, 1954 prescribes that any offence which is punishable by the ordinary criminal law of the State is also an offence against Military Law.
   
   c. Section 168 of the Defence Act, 1954 prescribes that the contravention of regulations, orders or instructions published for the general information and guidance of the Defence Forces by any act or omission is an offence against Military Law.
d. Actions on encountering a comment, post, tweet, blog, message, shared post, etc. that contravenes this document:

(1) Immediately inform the individual concerned that it goes against the social media instruction and ask them to remove/delete it as it may be a genuine mistake.

(2) If they refuse to do so, report it immediately to the Military Police or Brigade/Formation Press Officer, who will in turn contact the Military Police for further action.
Annex A

Can I utilise the information? (personal data, images, video, etc.)

Information was acquired by official means
Official: Photographer/videographer pre-designated by IC
Unofficial: Taken informally on a personal device

Were non-DF individuals briefed on recording information prior

Consent was given by all identifiable the individuals

The information cannot be utilised

The information can be utilised for official Defence Forces purposes

Are they serving members of the Defence Forces?

No issues were brought to your attention in relation to the information

Is the information accurate, appropriate and apolitical?
THINK BEFORE YOU POST
Anybody could be watching!

OPSEC, It only takes a moment!