



Ministry  
of Defence

Our Ref: FOI2021/08924

Ministry of Defence  
Main Building  
Whitehall  
London SW1A 2HB  
United Kingdom

Telephone [MOD]: 020 7218 9000

E-mail: DDC-  
SecretariatParliamentary@mod.gov  
.uk

[REDACTED]  
E-mail: [REDACTED]

24 August 2021

Dear [REDACTED]

Further to my reply to you of 4 August you have subsequently submitted a follow up request asked for the following information:

*“Thank you for your response and the revised documents.*

*I appreciate the lengths you have gone to here, however, I have reason to believe that the social media policies provided for the Royal Navy and RAF are not the personnel social media policies.*

*These appear to be the community “house rules” or terms of engagement for ordinary members of the public using MoD social media channels.*

*Could you please provide the social media policy/policies that RAF and RN personnel are obliged to follow?”*

I am treating your correspondence as a request for information under the Freedom of Information Act 2000 (FOIA).

A search for the information you requested has been carried out and I can confirm that the Ministry of Defence does hold information within the scope of your request.

Please see attached at Annex A the information requested in respect of the RAF Social Media policy. Section 40(2) has been applied to some of the information to protect personal information as governed by the Data Protection Act 1998. Section 40 is an absolute exemption and there is therefore no requirement to consider the public interest in deciding to withhold the information

The information requested for the Royal Navy is exempt under Section 21 of the FOIA (Information reasonably accessible to the applicant by other means). Section 21 is an absolute exemption and is therefore not subject to a public interest test.

Under Section 16 (Advice and Assistance) the information requested for Social Media advice/guidance/policy for RN personnel to follow is laid down in BR 3(1) 'Naval Personnel Management' Chapter 21, Article 2144 and Annex 21N. This is readily available in the public domain and can be accessed via the following external link:

<https://www.royalnavy.mod.uk/-/media/royal-navy-responsive/documents/reference-library/br-3-vol-1/chapter-21.pdf>

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail [CIO-FOI-IR@mod.gov.uk](mailto:CIO-FOI-IR@mod.gov.uk)). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

DDC Secretariat Parliamentary

## SOCIAL MEDIA POLICY FOR THE ROYAL AIR FORCE

Sponsor: DACOS Media & Comms

Liaison: M&C Senior Digital Manager

01 February 2019

### Aim

1. To provide clear direction on the rules and requirements of using social media for personal<sup>1</sup> and official<sup>2</sup> purposes. Guidance is given in this document to promote use of social media in a responsible way that will maximise our engagement with external audiences. It also provides guidance to all personnel using social media in a personal capacity. This document applies equally to all RAF personnel and civil servants whenever they use social media.

### Introduction

2. Use of social media allows us to communicate with the public outside of the organisation. It helps us monitor sentiment, identify key influencers, provides channels through which to deliver our messages directly to target audiences and influence beyond traditional audiences. It also allows closer engagement with our stakeholders.

3. The RAF encourages use of social media where it can add value and is within security and communications guidelines. All official accounts must be authorised by Air M&C. Care should be taken when mentioning RAF issues on personal accounts or when commenting on official posts. Individuals can be held accountable for information posted on personal accounts which may bring the RAF into disrepute.

4. This policy should be read in conjunction with:

- a. [2016DIN03-029: Contact with the Media and Communicating in Public](#)
- b. [Royal Air Force Brand Guidelines](#) (Defence Brand Portal account required)
- c. [A guide to social media behaviour for commanders](#)
- d. Royal Air Force Social Media Brand Guidelines (link TBC)

5. This policy covers:

- a. [OPSEC and PERSEC](#)
- b. [Direction and Guidance](#)
- c. [Online Security](#)
- d. [Setting up Accounts](#)
- e. [Changing Ownership of Accounts](#)
- f. [Evaluation and Support](#)
- g. [Closing channels](#)

---

<sup>1</sup> Accounts that are operated by individuals outside of their official duties.

<sup>2</sup> Accounts approved by Air M&C for official promotion of the RAF.

## **OPSEC and PERSEC**

6. OPSEC<sup>3</sup> and [PERSEC](#) must be considered at all times. The rules for 'Offline content' apply equally online.

7. Information posted on social networks may result in risks to personal safety. Care should be taken when sharing or posting both personally and officially on social media. Whether using an official or personal account be cautious about posting detailed personal information. For example, you should never mention your security clearance online. For more on staying safe online, see the "[Think Before you share](#)" guidance on the GOV.UK website.

8. Approval including retrospective approval must be gained for all official social media accounts through Air M&C. Accounts will be reviewed for content and suitability. Part of this approval process is to provide the correct training for users. Where such accounts have not been given approval they risk being closed down.

## **Direction & Guidance**

9. Failure to follow this guidance and inappropriate use of official social media accounts could be considered misconduct and could result in administrative action.

10. Users should not say anything on social media that would not be said on any other public channel; this means contradicting HMG policy or being politically partial, bringing the RAF into disrepute, divulging classified information, taking part in illegal or inappropriate behaviour, or breaching the terms of your employment in any other way on an official or personal account.

11. If users are granted a social media account, be aware that any activity within the PJHQ area of responsibility will require clearance through the [PJHQ media team](#) before release on any social media channel.

12. Figure 1 below is a framework to follow when clearance should be sought from Air M&C Digital before publishing content on official channels:

---

<sup>3</sup> JSP 440 Vol 5 Sect 6 Chp 6

Figure 1

<b>Go ahead</b>	Content from within your area of responsibility.
<b>Seek guidance from Air M&amp;C/PJHQ</b>	<p>Breaking news within your area of responsibility where there is no press line.</p> <p>The interpretation of a change of policy where the line is being agreed.</p> <p>Any activity within PJHQ OpCom/ Con</p> <p>VIP/ Ministerial movements.</p> <p>Rebuttal.</p>
<b>Don't do it</b>	<p>Subjects not in your area of expertise or direct responsibility.</p> <p>Any classified data.</p>

13. When sharing images you must consider OPSEC and PERSEC at all times. Where an image is of an individual you must ensure they have completed the MOD release form<sup>4</sup> if they are identifiable in the photo.

14. You can share interesting third party content e.g. media articles, NGO blogs, foreign partner military information etc. but only if you are sure that it is appropriate and it is politically impartial.

15. Take into account cultural sensitivities and avoid posting anything that could be considered offensive by anyone who may see the page (including audiences from other countries).

16. Debate is good, a protracted online argument is not. Take discussion best dealt with in private offline. We cannot argue online, nor play devil's advocate. We can only replace error with fact: this must be done in a professional and non-confrontational manner.

17. The account should not be used for directed surveillance of an individual or group. Directed surveillance is covert but not intrusive, is for a specific purpose, and is likely to obtain private information and is carried out other than by way of immediate response to events and circumstances.

18. Do not post or share anything which breaches copyright or that could be construed as advertising or promoting a commercial company. If in doubt seek advice through your chain of command.

19. Do not disclose information that is classified or privileged, or that may put you or your colleagues at risk, whether from crime, terrorism, or espionage.

20. Death in service should not be reported on any channels, nor should personnel respond to external social media posts. Permission should be sought from DDC through Air M&C first.

21. As with any form of communication, if in doubt, seek advice or do not post at all. Due to operational requirements there may be occasions when Air M&C direct that all posts cease for a given period.

<sup>4</sup> DIN 2017DIN05-006: MOD Consent Form

## Support and Training

22. Training is available for those that need support when using official social media. This support and training will be provided by Air M&C or DDC, or in some cases training will be provided through JIAG's Defence Communicators Course.

## Constant Review

23. Once a new account has been authorised, it will be subject to a 6 month probation period to assess its effectiveness. If this cannot be demonstrated, the channel may be closed. Accounts will be subject to an annual audit. Account owners are required to complete an assessment at Annex B to evaluate their account and return to Air M&C. If this evaluation is not completed, the channel may be closed.

## Online Security

24. All means of accessing an official social media account should use two-factor authentication. In many cases this will involve adding this level of security to your personal account that you use to access the channel. If you haven't done this before, please Google 'two factor authentication' and 'Twitter', 'Facebook', 'Instagram' or the channel you wish to run.

25. Twitter, Facebook and Instagram (which is part of Facebook) will 'verify' some important accounts, ones that are likely to be subject to impersonators, and celebrities and brands. Air M&C can approach Twitter or the other channels to get the account verified after launch if this is appropriate.

26. The following principles should be considered when establishing a social media account to minimise the likelihood of compromise:

- a. **Limit the number of people that have access to your account.**
- b. **Create Strong Passwords.** Generate a strong password, have mechanism to routinely change the password and hold it in a secure location.
- c. **Use Login Verifications.** Use 2 factor authentication to reduce the likelihood that your account can be hacked. This may also give you indications if someone is trying to access your account.
- d. Make sure your computer and operating system is up to date with the most recent patches, upgrades and anti-virus software.
- e. **Watch Out for Phishing.** You will get inundated with phishing e-mails, often mimicking or pertaining to be from various social media channels; the intent behind many of these is to get you to share your password. If in doubt delete the e-mail.
- f. **Suspicious Links.** Watch out for suspicious links, and always make sure you're actually on the social media channel in question before you enter your login information.
- g. **Be Wary of 3rd-Party Apps & Websites.** If you plan to use a social media channel to register 3<sup>rd</sup>-party websites or apps, be cautious as this may give the apps (legitimate or nefarious) access to your account. You are advised to not use the any account to register 3<sup>rd</sup> party websites.
- h. **Log out of active sessions.** If you connect to your social media account on a public computer, remember to log out when you are finished using it. It is an easy and highly effective step to protect your privacy.
- i. **Pay attention to DMs.** The most common way of infecting a Twitter account is via

direct message (DM). To avoid falling into that trap, the first thing you have to do is never open a message from an unknown sender. If the message claims to come from a friend, check its content first. Pay special attention to shortened URLs as they don't indicate what type of website they are taking you to.

j. **Conspicuous behavior of your contacts.** If, for example, one of your contacts starts tweeting in a foreign language, sending strange direct messages or acting weird, let them know immediately and suggest that they follow the aforementioned tips.

k. **Use a VPN.** If the your social media account is accessed through non-trusted networks, then a VPN should be used to protect your information, login credentials etc.

27. A local SOP should be developed for the operation of the account, which must include actions when it is suspected that the social media account has been compromised and should include the following basic steps:

a. If the account has been compromised the password should be changed and Air M&C informed.

b. For Twitter check the apps that have access to it and make sure they are all trusted. Any apps of unknown origin should be deleted immediately.

## Setting up Accounts

28. To apply for a new social media account for a station, squadron, team or an individual the application form at Annex A should be completed. The form should be returned to [Air M&C Digital](#) for approval.

29. Accounts will need to meet [the criteria](#) set out before they will be considered. Air M&C Digital will consider how the application fits into the wider range of channels available, and will make an assessment based on the wider audience need.

30. Only Air M&C Digital are to set up social media accounts and are to remain as Admin on Facebook pages. This includes all RAF related accounts such as stations, sports teams and station commanders.

31. All accounts are to comply with the RAF Brand Guidelines.

## Social Media Considerations

32. Running a social media channel consumes resource in time. We need to be clear about why accounts are being created, and what business benefit these will bring the organisation. We also need to know what success will look like for the channel, so we can effectively evaluate. The following factors should be taken into account when setting up a new account:

a. **Communication objectives need to be SMART:** Objectives need to be Specific, Measurable, Achievable, Realistic and Timebound, and need to link in with wider policy objectives.

b. **Recruiting:** Aiding recruitment can be a fair objective, but the channel will need to fit in with existing recruiting channels. The measure of success for this channel should be an increase in recruitment rather than simply engagement on the channel itself.

c. **Community support (external or internal):** Creating, and engaging with an audience is a good objective, so long as it brings other benefits that can be measured. It is not an end in itself.

- d. **Fixed-term or event/project:** Social media accounts should be created for permanent use. Channels should not be created for specific one-off events. Event pages on Facebook should be considered for these instances instead.
- e. **Customer service:** Channels can be created to meet the needs of specific customer audiences. Channels of this type may require more resources to meet the expectations of the audience (for example, some form of out-of-hours cover).
- f. **News and features:** A large number of successful pages already exist in the area of sharing news and features with our audiences. Any proposals for a new channel of this type need to have particularly strong evidence of both a quantity of content that would swamp an existing page, and a particularly high standard of quality, or a clear regional/specialist demand.
- g. **Awareness-raising:** "Raising awareness" of a particular subject is not a strong enough objective. What is the reason we would want to raise awareness? How does this activity link in with policy objectives?
- h. **Monitoring of individuals:** Accounts must not be used to target or monitor individuals' behaviours or activities online. Such activity – sometimes referred to as Open Source Intelligence (OSINT) – is subject to a number of legal and policy issues, and such activities must only be undertaken with the approval of the Chain of Command and by qualified staff. For further details, please contact the Air Principal Security Advisor (PSyA). This does not prevent accounts being used to investigate and confirm issues that are reported to the MOD, whether internally or externally, about content on social media.

## Social Media Activity

- 33. We do not expect everyone to use social media in the same way, but we do expect social media to be a core part of the toolkit of a modern communicator.
- 34. Social media can be utilised in these main ways:
  - a. Listening – following discussions, keeping track of news and building networks as part of day to day work.
    - (1) This means setting up an account with a monitoring tool (some of which do not require a social media account). You should also consider using digital tools that aggregate real time news trends from social and mainstream media. If you need further guidance on this, please speak to Air M&C. Examples of free tools include Tweetdeck or Hootsuite. You do not necessarily need social media accounts to use monitoring tools.
  - b. Low-key work related activity such as following influencers:
    - (1) You do not need permission to use social media accounts for low-key activity, officially or unofficially, but you should inform your MCO or Air M&C that you are doing so. You will need to take MOD security considerations into account.
    - (2) Examples of engagement on personal channels could include highlighting public information or relevant RAF events.
    - (3) Personal accounts should NOT be used for announcements, engagement, engaging in controversy, or breaking news – that is the job of official accounts. In the case of Facebook, this should be a page rather than a profile, even if it is generic.



(4) If you are concerned that a post may be controversial, please speak to your MCO or Air M&C.

c. Those in roles where active engagement and communication will be essential should use an official RAF branded channel. This could be personal (e.g. "Wing Commander John Smith") or corporate (e.g. RAF Recruitment).

## Changing Ownership of Accounts

35. If channel needs to change ownership, it's the responsibility of the current owner to ensure:

- a. There is a new, named contact / owner for the channel and this has been provided to Air M&C to update records and move the account to a new name
- b. The new owner of the account either is appropriately skilled, or has an assessment of training required and knows how to get it.
- c. The new owner is clear on the audience, objectives and plans for the page and how to collect and post content.

## Evaluation and Support

36. We need to demonstrate that social media is effective at meeting the agreed objectives. [Find out more about evaluation on the pages for the Government Communication Service](#). A template for evaluation is included in Annex B.

37. For existing accounts, support will be given to improve the quality of content to help make sure it continues to meet objectives. There are existing online support communities that eligible individuals such as channel managers are welcome to participate in, such as the Air M&C Digital "Slack" group.

38. Those who do a large amount of work on social media channels may wish to attend the Defence Digital Communications Group if they don't already do so. This group is where policy for the whole of defence online is discussed and set, and is a useful forum for sharing experiences, getting examples of good practice, and getting advice from communications experts both internally, and externally. If you wish to attend, speak to Air M&C Digital.

## Reasons for Closing Accounts

39. Social media accounts may be closed for the following reasons:

- a. Not being maintained / no evaluation provided.
- b. Not maintaining contact with Air M&C.
- c. No registered contact / owner.
- d. No longer required.
- e. Ongoing failure to meet objectives.

40. When a channel has outlived its time and needs to be closed the process should be:

a. Post to the channel explaining that the channel is going to be closed, posting a link to other, existing channels that might be suitable for the same audience. This should be done twice in at least a week-long period, naming a specific date when the channel will close.

b. On the day of close down work with Air M&C to hide or unpublish the page to ensure we keep the username.

41. Review of policy 01 Feb 2020.

**SOCIAL MEDIA ACCOUNT REQUEST FORM**

1. This form should be used to apply for all official RAF social media accounts. This includes corporate accounts (e.g. a Facebook page for a station) or an individual account (e.g. using your name & job title for a Twitter account).
2. If you have an MCO/PRO they must be made aware of this application.
3. More information is available via [MOD social media guidance](#)
4. If you have any questions, please speak to your MCO/PRO or the Air M&C Digital team about your application.
5. Your CO should approve the application before sending to the Air M&C Digital team at Air Command for consideration at **Section 40**.

<b>Applicant name</b>	
<b>Email address</b>	
<b>Establishment or unit</b>	
<b>Which social media tool is the application for?</b>	
<b>What would the name of the account be?</b>	
<b>What are your objectives for the account?</b>	
<b>Who is your target audience?</b>	
<b>What monitoring will you be doing?</b>	
<b>What conversations do you plan to engage in?</b>	
<b>Which strategic objective(s) does this support?</b>	
<b>Do you have the resource to make regular contributions?</b>	
<b>Please give an indication of how often you would post.</b>	
<b>How will you measure the success of this account?</b>	
<b>Are there are risks to opening this account?</b>	
<b>Is the management of this account included in your crisis handling plan?</b>	
<b>MCO/PRO or CO approval (and comment if appropriate)</b>	
<b>Air M&amp;C Digital team comment &amp; decision</b>	

**SOCIAL MEDIA CHANNEL EVALUATION SHEET**

<b>What theme(s) of the Defence Communication Strategy will your channel(s) support?</b>	
<b>What is the Policy Objective(s)?</b>	
<b>What is your SMART Communications Objective?</b>	
<b>Who are you targeting?</b>	
<b>INPUTS</b>	<ul style="list-style-type: none"> <li>* OASIS key steps (planning, baseline)</li> <li>* Costs (staff, staff hours, agencies)</li> <li>* Content schedule</li> <li>* Channel/platform selection</li> <li>* Pre-engagement activities (e.g. influencers, partners, suppliers)</li> </ul>
<b>OUTPUTS</b>	<ul style="list-style-type: none"> <li>* Multimedia publishing (e.g. blog posts, tweets, impressions, video, graphics, pics, page, audio, reach)</li> <li>* Digital channels (e.g. social channels, yours and others)</li> <li>* Reach (e.g. message penetration, share of voice)</li> <li>* Unique people reached for Facebook</li> <li>* Av. reach per each organic post</li> <li>* Ave. actual impression per tweet (or sum of followers)</li> </ul>
<b>OUTTAKES</b>	<ul style="list-style-type: none"> <li>* Follows, Likes, Shares, Retweets</li> <li>* Click-throughs, repeat visits, engagement rates</li> <li>* Bookmarks, Votes, Pins, @mentions, Hashtag use</li> <li>* Message sentiment, favourability</li> <li>* Comments (e.g. blog post, Facebook/Linkedin)</li> </ul>
<b>OUTCOMES</b>	<ul style="list-style-type: none"> <li>* Advocacy (endorsements, reviews, hashtag reuse, organic posts)</li> <li>* Co-operation, support</li> <li>* Referral traffic</li> <li>* Attitude or behaviour change</li> <li>* Satisfaction rating</li> <li>* ROI or BCR</li> </ul>
<b>ORGANISATIONAL IMPACT</b>	<ul style="list-style-type: none"> <li>* Contributions to Organisation Goals/KPIs</li> <li>* Behavioural (e.g. complying actions improvements)</li> <li>* Attitudinal (e.g. perception levels)</li> <li>* Experiential (e.g. customer experience)</li> <li>* Financial (e.g. increase revenue or cost reduction)</li> <li>* Reputation (e.g. public polling, internal polling)</li> </ul>
<b>CONTEXT</b>	Narrative statement: include any external and internal factors that have in some way affected your KPI

	Baseline	Review Point 1	Review Point 2	Review Point 3	End of Campaign
KPIs					
Data					