

## Considerations for Social Media

Even a restricted online profile, visible only to 'friends', can be easily accessed by uninvited third parties. This applies to private messaging services such as WhatsApp or Facebook Messenger as well.

Turn off automatic geo-tagging on devices to prevent your location from being revealed unless you want it to be.

Think carefully about if you want photos of yourself in uniform on your account, and what might be in the background of those photos.

Stop posting in the event of a major incident, especially if colleagues have been injured or killed or if 'Op MINIMISE' has been imposed.

Do not expect anonymity even if using a pseudonym for your account. Consider how a third party might read or use your posts.

You may be held responsible for communications in cyberspace, on the Internet or in social media, even if those communications go beyond the audience/ recipients you intended.

Read other posts carefully before liking, re-posting or responding to them. Be on the look-out for 'fake news' and phishing.

Regularly check and update your social media settings. When apps or software update, they often reset to default settings.

Don't access your social media accounts on MOD devices. If you think you are posting something worthy of being re-posted on the RAF's Official channels, let your unit media representative know.

Be upfront if you make a mistake online. It is virtually impossible to take something back, even if you delete it quickly, so it is best to tell your boss if you have got it wrong.

Help colleagues by looking out for inappropriate posts, tweets etc.

If you think someone should take something down, message them privately instead of drawing attention to it publicly.

If you set up an anonymous account or use a pseudonym you still must follow all the guidance above. It is not safe to assume anonymity.

### REMEMBER:

If you have any questions on these points, or what you should be doing, contact Air Media & Comms, your Command Chain or Media and Comms Officer:

Only access your personal social media accounts on your personal device rather than one issued by the MOD. If you think you are posting something worthy of being re-posted on the RAF's official channels, let your MCO know.

Online defence forums have international reach and are monitored by other military and journalists. Assume that any posts you make will be picked up, re-posted and aired on mainstream channels. Anonymity is not a safe assumption.

While you are not responsible for content posted by online groups that you are a member of, inappropriate content can be linked to you and then to the RAF. The RAF supports you if you stand up for our message online, but it is better never to be associated with inappropriate content.

Be upfront if you make a mistake online. It is virtually impossible to take something back, even if you delete it quickly, so it is best to tell your "boss" or line manager if you have got it wrong.

Help colleagues by looking out for inappropriate posts, tweets etc. If you think someone should take something down, message them privately instead of drawing attention to it publicly.

If you set up an anonymous personal account or use a pseudonym you must still follow all the guidance within this policy.

Do not create fake accounts to impersonate other people, it breaks social media site rules and is against MOD policy.

Think carefully before indicating on online profiles such as social networks or dating sites that you are in the RAF. However, if you choose to be public, the RAF fully supports anyone who contributes positively to our overall digital presence.

Whether your profile indicates that you are in the RAF or not, your posts and videos must always abide by our Values & Standards and be clear that you are not communicating on behalf of the RAF in an official capacity.

### REMEMBER:

The RAF is a national institution that protects the UK; its reputation must be looked after to preserve its credibility as a fighting force, its freedom to operate and its attractiveness as a modern employer that fulfils its people's potential.

For more information see - 2014DIN03-24

## Social Media for RAF Personnel

### Why?

Online conversations about the Royal Air Force take place every day, and we want our personnel and the RAF family to be able to join those conversations. Our people represent the RAF online, and can share the optimistic and positive ethos of our organisation that many don't get to experience first-hand. We have a great story to tell and should be prepared to positively engage on social media.

Think carefully before indicating on online profiles such as social networks or dating sites that you are in the RAF. However, if you choose to be public, the RAF fully supports anyone who contributes positively to our overall digital presence.

Our role in the social media community is to explain what we do and help inspire the next generation Air Force as well as act as brand ambassadors for the RAF. This social media policy should guide your participation online both personally as well as when acting in an official capacity on behalf of the RAF.

### Who?

This policy applies to all members of the whole force, whether on duty or off duty, whenever they use social media.

Whole Force includes:

- RAF personnel - from Air Chief Marshal to Aircraftsman
- Civil Servants - all grades
- Contractors employed directly by the RAF

For military personnel, online comments and content should reflect the core values and standards laid down in AP1. For Civil Servants working for the RAF, online behaviour is subject to the Civil Service Code. Whilst the Royal Air Force supports personnel who choose to use social media to communicate their life in service, all Service personnel and Civil Servants should be absolutely clear that they can be held to account for poor online behaviour. Comments made online are viewed the same as normal verbal communications, this includes making comments on any online 'forum', official or not including making comments on our sister Services accounts.

If you are victim of online abuse or see online abuse being carried out by other Service Personnel (RN and Army included) or Civil Servants, take a screen shot and pass this on to your Chain of Command and/or P1 Team.

# Social Media for RAF Personnel



## Do's and Don'ts regarding Social Media. Be smart, if in doubt ask an expert

Any material posted on social media is classed as 'Communicating in Public'. Social media includes sites such as: Facebook, LinkedIn, Twitter, Instagram, Flickr, You Tube, blogs, chat rooms, or similar social media forums.

**You CAN:** participate in unofficial social media forums, unless you are of certain Special Employment Groups. However, **Do Not** use social media forums to vent your frustrations, grievances and concerns on Service matters, in particular on Official RAF Channels as this immediately damages the RAF's reputation. If in doubt seek advice from your chain of command.

### 'Private' Messaging Communications

**Do** continue to use email and person-to-person messaging apps to discuss aspects of Service life.

**Don't** use person-to-person messaging (including Whatsapp and SMS) to discuss or send OFFICIAL Defence information without appropriate authorisation.

### What you Can and Can't post on Social Media and the Internet

**You Can** take photographs in authorised spaces and during public events (subject to local controls).

**You Can** post photographs taken during public events if members of the public are allowed to take photographs.

**You Can** say where you are now (subject to local control), but not for how long, if this is attached to your unit's movements.

**You Can't** post photographs taken inside aircraft, or an aircraft undergoing maintenance without official approval.

**You Can't** post content which may cause offence, bring the Service into disrepute or bring superiors into contempt.

**You Can't** post anything relating to the movement of personnel, unless it has already taken place.

**You Can't** say where you are going to be in the future if this is attached to your unit's movements.

**You Can't** point out security or technological limitations.

**You Can't** indicate your, or anyone else's Security Clearance level.

**You Can't** compromise, or post classified material, including official passes.

