# Social Media is Changing the Face of Defence

Social media has helped the world gain a greater understanding of the role of the UK Armed Forces. Many people across the military use social media, and it can have a positive effect in raising awareness across the globe.

The use of social media is allowed and, when used appropriately, is encouraged. You do not “have” to use social media.

**The issue we face is not why or how we use social media, but how well we use it.**

This guide tells you what is and isn’t acceptable behaviour for military personnel on social media.

For information on how to use these channels and, in particular, how to fix your personal security settings, visit www.blogs.mod.uk/onlinesecurity


# Your Account Security

Think about who can see your account. Security settings can be adjusted on all major social media networks. Do not post personal details such as your address, telephone number, bank details etc. These may make you, your friends and family a target.

Without the right security settings in place you are opening up anything you post to everyone - from journalists to criminals or terrorists.

**It may not just be friends and family reading your status updates.**

# Acceptable Behaviour

All Defence personnel follow the **core values** of their Service or organisation. We should be honest, objective and act with integrity at all times.

Offline or online, on duty or off duty, we should always behave in a lawful, appropriate and professional manner, wherever we are in the world.

# Using Social Media...

There are several ways we can use social media. Whatever context, you are an **ambassador** for Defence.

## ...in a Personal Context

If you share photos of yourself (and mates) in uniform, refer to your Service or organisation (by insignia, flash or logo), it will be obvious you are a member of the Armed Forces or a Defence civil servant. People will relate what you say to your Service, even if you state your opinions are your own.

Make sure your family and friends are also aware of the risks. It is not only you who can share sensitive information.

**How personal do you want your profile to be?**

### Do you know when you have crossed the line?

- **What if this ends up on the front page of the papers?**
- **Would I say this to my CO in front of 100 people?**
- **Would I leave this information lying on a park bench?**
- **What if a terrorist or criminal gets this information?**

**What you say online stays online. Forever.**

## ...in a Professional Context

In social media this refers to speaking through an official corporate presence, for example your unit, your Service or Defence. You could be the person who posts something on behalf of your unit or Service.

All material must be cleared in advance before it becomes a public record and must therefore be in line with what your Service or unit is trying to achieve.

## ...in a Sponsored Context

Speaking in a sponsored context means being a representative speaking through an official channel. You can post as yourself but must have support of your Service or Defence. Speak to your unit commander and unit press officer/local security staff who will advise you on what to do, e.g. create a blog.

## GREEN

There are many things that you can share on social media. However, you should:

- Be aware of who can see your account. Are your settings set to 'private'? Is your content proper?
- Be polite, constructive and honest. Be a credit to your Service.
- Be sure you know the difference between fact and opinion.
- Be quick to refer to official channels or spokespeople about official matters.
- Be sure to protect the privacy of your family and friends as carefully as your own.
- Be aware that quality is more important than quantity. It's better to have fewer, good-quality articles and posts than lots of bad ones.
- Be aware of the policies set out by your own Service.

**It may not just be friends and family reading your status updates.**

The use of social media is allowed and, when used appropriately, is encouraged.

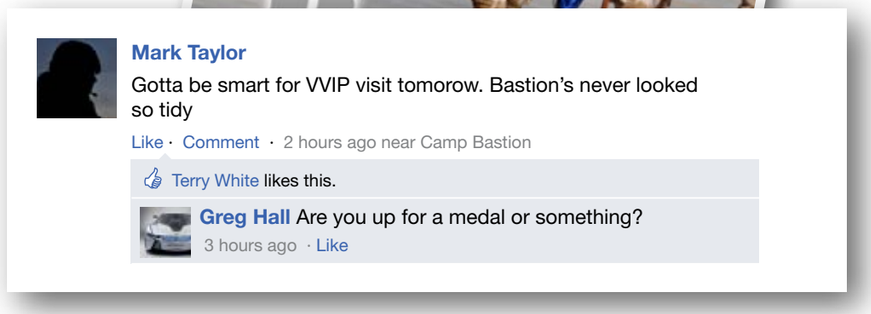
The issue is not why or how we use social media but **how well** we use it.

This guide tells you what is and isn't acceptable social media behaviour for military personnel.

## AMBER

Always seek permission if your post may:

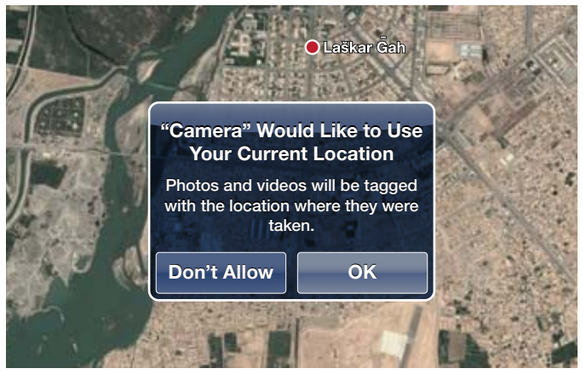
- Relate to operations or deployments.
- Seem to offer opinion on Defence and Armed Forces activity. Stay in your lane.
- Be mis-interpreted as speaking, on behalf of your Service or the MOD.
- Relate to controversial, sensitive or political matters.


## RED

- Do not breach OPSEC or PERSEC by giving away sensitive information obtained through work, such as troop movements, capabilities or shortfalls, exercises, etc.
- Do not embarrass or bring your Service or Defence into disrepute. This includes sharing any offensive or sensitive materials.
- Do not share any official Defence information that you are not authorised to share.
- Do not complain about Defence policy or make political statements in any public forum, if it looks like you are speaking officially. Raise problems through your chain of command.
- Do not reveal your exact location on operations. Ensure location services and geo-tagging features are off.
- Do not write anything out of anger, spite, over-reacting or when drunk.
- Do not be a bully or discriminate.
- Do not steal someone else's content and post as your own, especially copyright material.

**Failure to follow these guidelines will result in DISCIPLINARY ACTION.**




ROYAL NAVY

ARMY

ROYAL AIR FORCE

Ministry of Defence

# Share?

**A guide to social media behaviour for personnel**

## Any Questions?

Here's where to go for more information.

### Who

Directorate Media and Communication

DMC-SecOnlineEngagement@mod.uk

### Where

www.blogs.mod.uk/onlinesecurity

Search 'Security Awareness Resources' on Defence Intranet