



**ROYAL
AIR FORCE**

Social media.



Let's keep it safe and responsible.



www.getsafeonline.org

Read our expert tips on the safe and secure use of social media

For millions of people around the world, using social media regularly has become second nature.

Social media has very many positive aspects, but also negative ones such as over-use, too much focus on other people's lives and, increasingly, fake news. It's also essential that on social media, you protect yourself and your family against fraudsters and abusers.

For the RAF and other branches of the military, social media also presents particular issues, such as serving personnel and their families oversharing sensitive information and innocently accepting friend requests from hostile actors. These and other situations could pose a real threat to RAF and national security.

Don't overshare

Consider what you share on social media and how it might impact on yourself, friends and loved ones, now or in the future. And remember that sharing sensitive information about locations, operations and deployments is not only strictly off limits, it could also compromise your family's safety.

Check your profile

Much of the information people commonly share in their profiles – such as date of birth, address, first school and other details – could be seen and used by fraudsters or hostile actors to glean your confidential information. Keep your profile information to a bare minimum.

Get familiar with features

Gain familiarity with features like Instagram Stories (where your posts that disappear after 24 hours could be screen grabbed) and Facebook Live (taking care what you stream because it *literally is live*).

Think before you post

Posting inappropriate comments, photos or videos could result in at best, embarrassment or at worst, physical danger to yourself, others or the military, now or in the future.
Post in haste, repent at leisure.

Check your privacy settings

Make sure only those you want to, can see your profile and posts. Even doing this is no guarantee that your information won't be passed on and seen by others. Review and set geolocation settings on apps and cameras so as not to broadcast your location. Don't use check-in features.

Following links

Links to free or low-cost offers, prize draws, investment opportunities, charity appeals, sensational news, surveys or quizzes could be either fraudulent, result in downloading spyware or take you to inappropriate or extreme content. Avoid clicking on such links.

Dealing with abuse

If you are subjected to abuse such as insults, trolling or stalking, block the perpetrator and report it to the platform and, if appropriate, the police. Also remember that behaving in this way yourself could be very hurtful to others.

Holiday posts and pics

Posting that you are away on a family holiday could advise a burglar that your home is unoccupied. Some insurance companies reject burglary claims based on social media activity, so think before you post or send.

Social media and your children

Disable geolocation in your kids' app settings – such as social media, maps and cameras – so they can't be tracked. Talk to them about who they accept as friends (stranger danger). Impose limits on how long they spend online and set a good example yourself. Remember that most social media sites have lower age limits for a reason.

Being influenced

Don't get swayed to do something you know is wrong, and don't try to influence others into inappropriate, irresponsible, dangerous or unlawful actions, including those that could bring the RAF into disrepute.

Learn how to spot fake news

Social media is a popular platform for fake news and celebrity profiles. Instigating and sharing fake news can be harmful, upsetting or dangerous, so do not get involved in this. Links in fake headlines or stories can also lead to fraudulent or malware-ridden websites.

Buying and selling

You can find anything from cars to holidays, trainers to festival tickets on social media marketplaces. Do all you can to check that ads are genuine, and never pay by direct bank transfer in case they are fraudulent, as you won't get your purchase or your money back.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector initiative backed by a number of law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit www.getsafeonline.org



www.getsafeonline.org

GET SAFE ONLINE: WORKING TOGETHER WITH...
