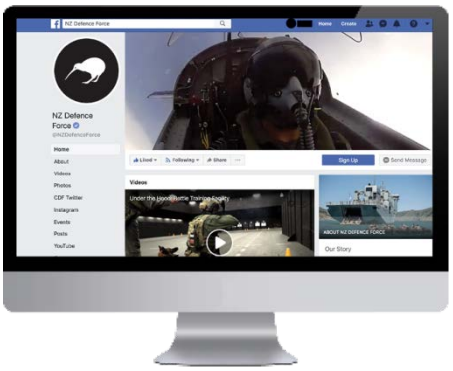

How to keep safe on

Facebook

Facebook can be great for keeping in touch and up-to-date with your family, friends and communities.

As with any social media tool, those benefits come with some risks that you need to be mindful of as a member of the New Zealand Defence Force.

To ensure that your use of Facebook doesn't pose a risk to you, your family, your mates and your employer, we've got six easy to remember principles to keep in mind when you're online.

Social media companies update their privacy and security settings fairly regularly. Updated 'How to keep safe guides' can be found in the DPA Toolbox on the Defence Public Affairs Intranet.

If you have any further questions or any feedback, please email **socialmedia@nzdf.mil.nz**

NZDF's six safety tips for Facebook

1. Facebook is forever

Even deleted content can live on in cyberspace. Don't post anything today that you wouldn't want to have to talk about with your CO tomorrow (or in ten years' time), and keep in mind that a poorly thought out post, like or share today might have implications for the security clearance you need for your next dream posting.

Any post or comment should be thought of as public. Even if it's in a private Group or chat, once it's on someone else's screen, you have no control over it.

2. Keep your privacy, security and advertising settings on lockdown

Facebook keeps showing us that they will share nearly anything with nearly anyone, unless you expressly tell them not to. Make sure you know what the different privacy, security, and advertising settings mean, and update them to keep your information, your location, your connections and your posts private.

To check what the public can see, go to 'Your profile' > Tap 'View' (best done on a desktop, not on a mobile device).

You can also use 'Facebook's Privacy Check-up' to review how you're sharing your information with people on Facebook and with the apps and websites from other companies that you've used Facebook to log into.

3. Update your password regularly

It's important to have a strong password and to update your password regularly.

Creating the right password will help keep others out. Make sure your password is unique, but memorable enough that you don't forget it. Don't use a password that you use on other sites – if one gets hacked and your password is stolen, hackers will often try it on other sites. You could have a set password but create variations. Don't share your password with anyone.

To change your password, go to 'More' > Tap 'Settings' > Tap 'Security and Login' > Tap 'Change Password' > Type your current password. Type your new password and re-enter it one more time, then tap 'Save Changes'. **Learn more:** www.facebook.com/about/basics/stay-safe-and-secure/passwords

To check your security and login details, go to the 'Settings' section of your profile > then tap 'Security and Login'.

4. Add two-factor authentication

Like any username/password access, your user access can be hacked. It's important you have your account locked down. Adding a two-factor authentication can be a good way to make sure no one, other than yourself, can access your account.

Adding two-factor authentication means that if you access your Facebook account from a new phone or computer, you'll be asked to enter a login approval code (which is sent to your cellphone). If someone other than you is trying to access your account, they won't be able to log in. **Learn more:** www.facebook.com/about/basics/stay-safe-and-secure/login-approvals

5. Tagging can be dangerous

You should update your privacy settings to stop people from tagging you. Leaving yourself open to being tagged makes it easier for others to track you online – putting you, your mates and sometimes even your mission at risk.

For the same reason, you should think twice before tagging others in posts, photos or comments. And have a talk to your family and friends about why they should avoid tagging or naming you in posts and comments – particularly comments on NZDF or Service Facebook Pages and Groups.

6. Protect your location

Facebook uses the location services on your phone or tablet to share more about who and where you are, both to your followers and their own advertisers. You should avoid adding location tags to your posts while at work (including exercises and operations).

To remove location tracking completely, turn off your location services. Go to 'Settings' > Tap 'Privacy' > tap 'Location Services' > scroll down and tap 'Facebook' > select 'Never'.

Some useful links

- Facebook privacy basics: www.facebook.com/about/basics
- Facebook's 'Stay Safe and Secure': www.facebook.com/about/basics/stay-safe-and-secure