New Zealand
DEFENCE
FORCE
Te Ope Kātua O Aotearoa

# Your handy guide on Social Media

**Version 1.0** | September 2019

A FORCE FOR
NEW ZEALAND

# Contents

# What is social media?

1

**Social media refers to online services that enable people to stay in touch, create and share content, and participate in a range of social activities online. Social media has become a part of most people's everyday communication.**

Even if you don't belong to a social network you may be involved with social media without realising.

Internet based platforms like Facebook, Twitter, YouTube and Instagram have given people new ways to share their lives and stay connected. For people separated by distance, they are invaluable – a Skype call when you are thousands of miles away from your loved ones can be a treasured moment – but social media has its downside too.

Social networks are designed to feel very personal but many of them are also very public, with news, information, images and opinions spreading instantaneously across networks and becoming accessible around the world.

Understanding the risks associated with social media and how to manage them will help you get the most out of the online tools and communities available to you.

**This handbook is designed to help you navigate the world of social media while keeping yourself, your family and your mates safe.**

2

# New Zealand Defence Force and social media

**The New Zealand Defence Force (NZDF) is active on several social platforms (particularly Facebook, Twitter, Instagram, LinkedIn and YouTube) and each of the three services, Navy, Army and Air Force, also have an active presence.**

We use Facebook groups to share news, information, events, photographs and videos with our communities. Each community has a specific interest – for example, it might be one of the Services, veterans or the RNZAF Black Falcons – and the Facebook pages help everyone keep in touch.

Because online technologies and how to best use them can change rapidly, NZDF has a dedicated Digital Channels team leading an expert approach to using social media and other online communications. Over time, the dominance of some of today's social media networks may change but the need to connect with our communities on the social platforms they use will remain the same.

The social media networks we engage with help us to share the NZDF story with people at home and abroad. We share good news – and bad news – and welcome comments and conversations.

**Follow us on social media:**

@NZDefenceForce

@NZNavy @NZArmy @NZAirForce

There are also many sites that mention or cite NZDF which are not 'official' – they have been created by people who are, or have been, involved with the NZDF in some way.

Running a presence on a social networking site takes time, effort and attention. It can also carry legal responsibilities as well as an obligation to protect NZDF's reputation. Don't rush off and set up a page or account yourself. Before setting up a group on Facebook or using a brand new channel, you must consult with Defence Public Affairs (DPA) (socialmedia@nzdf.mil.nz) to ensure that you are complying with DFI 0.70. DPA will ensure that you select the most appropriate option for you and will help you understand the risks and obligations associated with running a channel.

The NZDF social media channels have a large audience and are always keen to share what's happening in your community/unit/squadron. Get in touch with the team at socialmedia@nzdf.mil.nz or find out how you can submit content via the DPA's Intranet site.

**Looking to set up a new NZDF social media account?**

Before setting up a group on Facebook or using a brand new channel, you must consult with Defence Public Affairs (DPA) **socialmedia@nzdf.mil.nz**

3

# **Social media** and you

**Like most people, you'll probably be using social media primarily to stay in contact with family and friends.**

While your private posts and messages are unlikely to be read or viewed by those beyond your immediate circle of friends and followers, privacy settings on the social media networks can mean that even a 'private' post can 'go public' quite easily – and completely unintentionally. As a member of the NZDF, you need to be acutely aware of your privacy settings on every social media network that you use and understand how they work so that your messages and posts reach only those you intend them to reach.

Your comments and thoughts on other people's posts may automatically become public because others may not be as vigilant in their privacy settings as you are – so be careful with what you say. Not because the NZDF doesn't want you to engage, but because you might, unwittingly, put yourself and your mates at risk. Don't forget, everything can be screenshotted.

Developments in geolocation mean that social networks will, given permission, let people know where you are. You may have organised your privacy settings not to reveal your location but a simple act, such as failing to disable location services on your mobile phone, could let people know your position.

When engaging in social media exchanges, be aware that you continue to be subject to either the *Armed Forces Discipline Act* or the *Civil Code of Conduct*. These govern our conduct in all situations and are equally applicable to the social media environment.

# **Social media** and security

4

**The most important factor to remember when using social media is the need to maintain our operational security. Social media is a fast, evolving and effective means of distributing information and that means operational security should be at the forefront of your thoughts when engaging with others.**

NZDF personnel are allowed to use and belong to social media networks and platforms but implicit in that is the understanding that in doing so, they will not violate unit policy or the *Civil Code of Conduct*.

Even trivial information can be dangerous online for your mates and your loved ones. It could even get someone injured or killed. Piecing together information through the Internet is a surprisingly easy task and adversaries are very good at connecting pieces of information together by using the trail of information we leave online.

So, avoid mentioning your rank, locations, deployments, dates, names, equipment and other capabilities. Don't tag photos with locations, either deliberately or by accident, because your settings are incorrect. Another way to stay safe is to disable the GPS function on your smartphone and not use location based social media networks while you are on duty or deployed.

# 5 Social media and reputation

**Your online activity, particularly where you can be directly identified as a member of the New Zealand Defence Force, can have an effect not just on how you are seen, but also on how your Service and the New Zealand Defence Force are regarded.**

In extreme circumstances, poorly considered social media activity could result in legal ramifications for the NZDF or disciplinary actions against you and members of your team.

To manage these risks, keep your social media profiles locked down, and always use social media as if everything you do is public.

Always think twice before posting something and ask yourself how your CO would view the post in the cold light of day. Avoid posting any images that show NZDF personnel in uniform with alcohol visible.

Make sure you have approval to post things related to your work. Remember that there are official NZDF channels that might want photos or videos associated with your work, operated by experts in a position to ensure posts are suitable for publishing before they go online.

The need to think carefully about your social media activity also applies to how you interact with posts by others. Comments associated with NZDF and Service accounts can get passionate, with strongly held positions sometimes getting in the way of professionalism and civility. Likewise, comments between team mates on Service and NZDF posts can become overly familiar, using language and banter that is not appropriate in a public forum. These scenarios reflect on the NZDF and create a large amount of work for the team that manages those official channels.

Keep in mind that the Official Information Act 1982 applies to you when you represent NZDF on social media or if you use it during work time, for work purposes. This means that what you say or post online can be requested by the public or the media at any time.

The Harmful Digital Communications Act (HDCA) 2015 also applies to any content you post online, including through emails, texts, websites, apps or social media.

For more information on the HDCA, visit **netsafe.org.nz**

# 6 Staying safe online

**Visit DPA's Intranet for the most up-to-date versions of the 'How to keep safe on social media' guides.**

## 6.1 Social networks

Check out the 'How to' guides at the end of this handbook for tips on how to make sure your security and privacy settings on Facebook, Twitter, Snapchat and Instagram are locked down. For the most up-to-date versions, visit the social media hub on the DPA Intranet site.

## 6.2 Secure chat apps

So called secure chat apps such as WhatsApp and Messenger are designed to protect your messages from surveillance from third parties. These apps usually only permit users to communicate with others who have also downloaded the app.

In general, secure chat apps give users greater protection against eavesdropping by concealing identities or making the contents of the messages indecipherable to anyone except the intended recipient. As a result, using secure chat apps may offer users two layers of security when the app is in use – anonymity and data security.

However, as with any communication over the internet or a cellular network, your personal data and messages are potentially at risk of being compromised:

- App providers collect user content, contact lists, and usage information, and hold this information for an indefinite length of time. Some of this information may identify devices or users. Snapchat shares this information with affiliates and third parties
- Messages not encrypted from end-to-end can be intercepted and decrypted
- Messages can also be screenshotted and shared to a wider audience than intended
- App providers may choose to log user data for an indefinite amount of time. Data logging can allow the recovery of older communications
- Messages are only as secure as the device they're held on, if you or the person you're messaging have your device compromised, your messages are compromised

## 6.3 Online dating sites

Online dating services are used by people looking to develop relationships with other users. These sites usually require their users to create a public profile, which contains photos of themselves as well their personal information. These profiles are often searchable through the site and can be pushed to other users who share common interests or locations.

**Protect your web-based online dating profiles and associated personal data**

Online dating sites present a unique set of threats to users when compared to other social networking sites. They encourage interactions between unacquainted individuals, collect extensive personal information, and have only few methods of verifying the accuracy of users' claims. Before you sign up to online dating, you'll need to think about the following threats to your personal data:

- Sites use questionnaires to help connect like-minded individuals, allowing them to collect targeted information about users' lifestyles
- Most sites encourage users to connect a social media account (such as Facebook) to their profiles or require face photos to help verify the account's legitimacy
- Matches may request personal contact information (e.g. phone number or social networking service). Use the dating site's chat feature as the only form of communication
- Catfishing – when someone creates a fake identify online with the intent to pursue someone romantically under false pretences. Catfishing can lead to financial scams, identity theft, character defamation and other general online scams

***Tip:*** *Don't use a picture of yourself in your uniform as your profile picture. While you may get more interest from potential partners with a profile photo of you in your uniform, you also open yourself up to more scrutiny.*

## 6.4 Fitness trackers and apps

A fitness or activity tracker is a device that allows people to track their fitness-related metrics such as routes walked, run or cycled. It is usually a wearable device worn on the body. A common fitness tracker is a wristband that is worn all day.

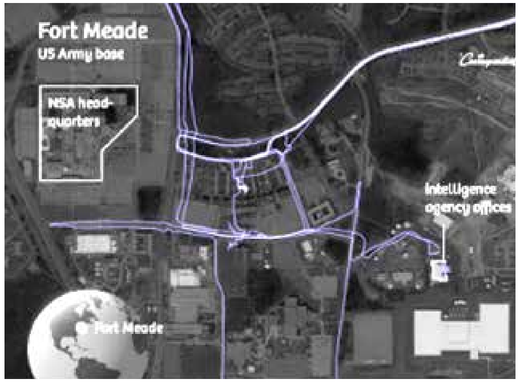
Most wearable fitness trackers are used for fitness, wellness, and sleep tracking. They all come with a smartphone or desktop app (such as Strava, Polar, Map My Ride) that provide the insights and metrics. A particular vulnerability of fitness trackers is that your data can establish your 'pattern of life' i.e. identifying your habitual movements and health data, leaving your activities exposed to third parties.

### Check your privacy settings

- If logging rides or runs, mark them as 'fun and fitness' rather than the more specific 'biked or run to/from work' or 'commute'
- If you're about to visit a sensitive site or work in sensitive areas, switch off the fitness app or fitness tracker. Turning on Flight Mode before approaching a sensitive area is an easy way to stop all geo-location functionality on your mobile phone
- If you must use a fitness app or sports watch, only turn it on once you're well away from your home or sensitive workplace
- Don't share your fitness data online
- When signing up to fitness apps either:
    - o don't use your real name or
    - o just use your first name and your initial for your surname i.e. Max T

**Case study**

### How a fitness app was used to identify military personnel



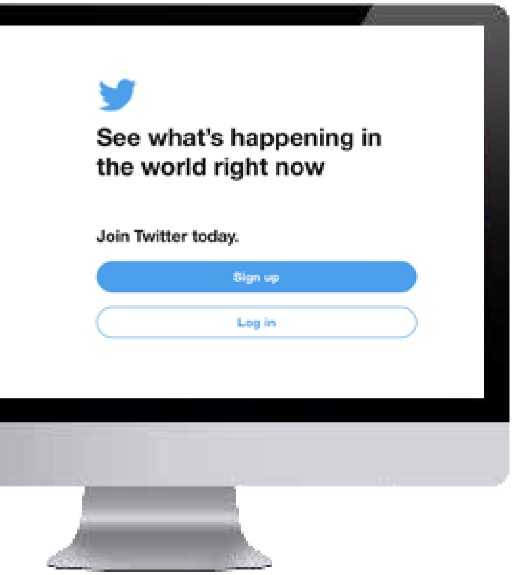
Movements logged via Polar fitness app at Fort Meade, USA

In July 2018, Dutch journalists published a story about how they used the fitness app 'Polar' to identify military personnel.

They started by looking at a military base – the app showed a run logged by a jogger who used his real name. They found other runs by this jogger that either started or ended at a house in a nearby town – likely to be his home. On LinkedIn they learned that he's a senior military officer – whose home address they now know. From here it didn't take much to find out details about his family.

The data in the app gave journalists a pathway to find out military personnel names, where they work, where they live and details about their families. There was even a Kiwi link – the article specifically mentioned that they had identified several NZ personnel who visited the NSA Headquarters in Fort Mead, USA.

Polar has since disabled its interactive map – but it's not the only fitness app out there. Any commercial app has the potential to expose your personal data, whether you've selected private mode or not. Can you really trust companies with your personal information?



See what's happening in the world right now

Join Twitter today.

## 6.5 Online registration

*Remember that even if you make your data private, the service still has access to your data and may share it with third-parties.*

- Avoid filling in the optional identity fields for online profiles; only fill in the minimum required
- Do not upload or share your existing contacts with a social network during registration
- Once you've completed the registration process, remove any identity data from your personal profile that was required during sign-up
- Change your privacy settings to protect your identity information immediately after registering

**John D.**

Instead of using your full last name, use your initial instead – especially if your surname is uncommon.

*Below are some tips to help minimise your exposure online when you sign up for a social network service:*

- **First and last name**
  First and last names are compulsory for most social media accounts. Where possible, instead of using your full last name, use your initial instead – especially if your surname is uncommon.
- **Username**
  Usernames are unique to each user account, and are used to identify individuals within a network. When making your username, do not include personal information such as your name, location, or birthday.

  Do not use the same password or username across multiple accounts. Use passwords that are complex and unique (include numbers and special characters).
- **Birthday**
  Birthdays are used to verify the user's age and customise age-appropriate content on the site. Make sure that you remove your birthday information from your public profile. Don't share your full birthdate unless it's required – you may want to consider using an incorrect birth day and month.
- **Address/location**
  Location information requirements may include address, city, postcode, and/or country. During sign up, only provide the most generic location level required, or consider entering a nearby postcode or city. Never give social network services your physical address.
- **Social login**
  Services may allow users to sign up through a pre-existing social media account (e.g. Facebook, Twitter). Avoid using social login whenever possible.
- **Mobile phone numbers**
  You may be asked to verify your identity using a mobile phone number. Either avoid using services that require phone numbers or opt to use an alternative method to verify your account.
- **Email address**
  It's almost guaranteed that you'll need to use an email account to sign up for a social network account. We recommend creating an email address solely for registering for social network accounts. **Never use your work email address.**

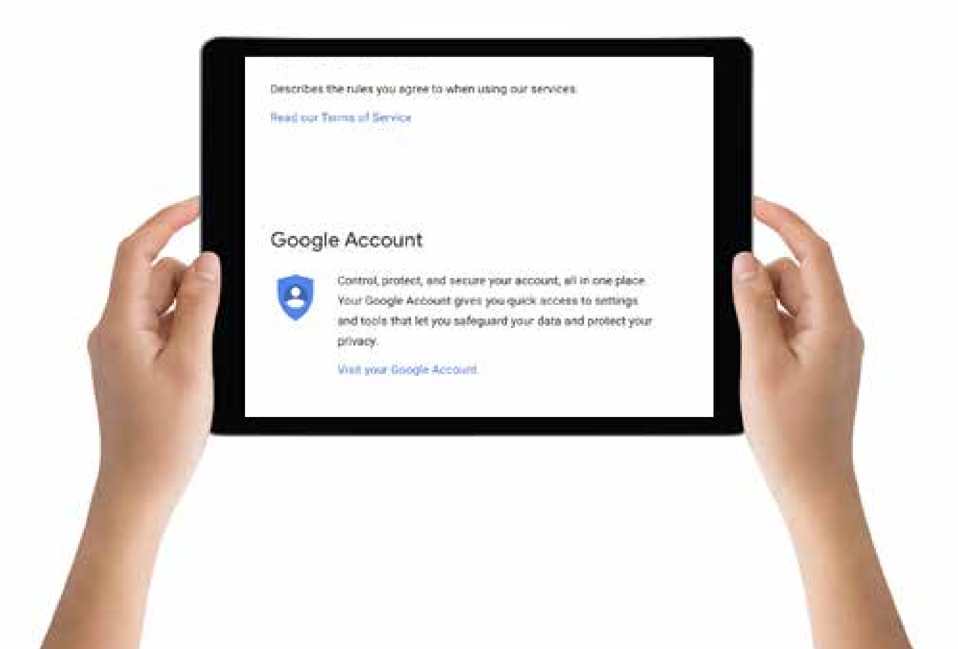
# 7 Keeping your device (smartphone, tablet) secure

**Here are some simple tips for keeping your device safe:**

- Protect your device with a password that uses a mixture of numbers and letters. Pattern locks can be strong but have a greater risk of being compromised. We recommend changing your passwords frequently (approximately every three months)
- If available, enable hard-disk encryption on your device. iPhones and Android devices with recent operating system upgrades may enable encryption by default
- Limit accessing sensitive information from the lock screen. For example: call logs, emails, text messages, and voice assistant functions (Siri, Google Now)
- Malicious emails and texts can infect your device with malware. Never click on links from people you don't know and regularly run antivirus software
- Cameras and microphones can be remotely activated. If you're having a sensitive conversation, make sure your device is in a different room
- If available, restrict permissions to limit the personal data apps can access. Check what data (e.g. location) the app collects before downloading it
- Immediately install smartphone operating system updates and security patches. Keep all apps updated to maximize protection
- Never jailbreak smartphones. Jailbroken phones allow malicious apps to bypass device security protocols and alter device software
- Only install apps from the official Apple or Google Play stores
- Record your devices IMEI number to identify device if lost/stolen:
  - iPhone: Settings > General > About
  - Android: Settings > About device > Status > IMEI information

***Note:** only tablets that have cellular capability will have an IMEI number*

- Always wipe the data on your device before discarding, donating, recycling, or selling it. Either transfer the SIM card to your new device or destroy it



Describes the rules you agree to when using our services.

Read our Terms of Service

Google Account

Control, protect, and secure your account, all in one place. Your Google Account gives you quick access to settings and tools that let you safeguard your data and protect your privacy.

Visit your Google Account

# 8

# Your 'stay safe online' checklist

- Sort out your privacy settings. If you play games online or through your social network, these can automatically tag you and post an update on the game to a friend's page. Disable this option not just on your device (mobile phone, laptop, PC) but also within the game settings
- Don't post sensitive information about where you are, what you are doing and who you are with
- Turn off GPS on your smartphone
- Review photos and videos before they go online – check them for anything that might reveal a sensitive location or your deployment. Turn off the ability for you to be tagged in posts and photos or, at the very least, turn on the review function. That way you can see what you've been tagged in before it goes public (and have the ability to stop it going public if need be). Protect your mates by not tagging them in images on main NZDF channels (see case study example on page 22)
- Talk to your family and friends about using social media and how too much detail posted online can be a problem. For example, a family member's post might read:

*"Missing Sally sooo much. She is going to be in Afghanistan at XYZ Camp near Bagram all Christmas – and not home for two months :( Really sad".*

Help them to understand that:

*"Sally is posted overseas this Christmas. Really sad but can't wait till she's home"*

is a better – and safer – option. A private message to Sally would be an even safer option

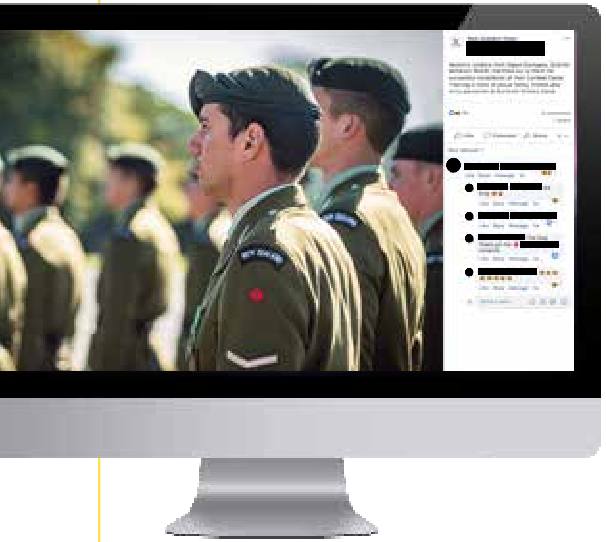
**Think before you post**

Are you happy with this update being available to all? Could it put yourself or others at risk, breach regulations or compromise your role as a Defence Force professional?

- Conduct your online relationships in the same way that you conduct yourself offline. Speak to people you work with in a professional way, particularly if you are in a leadership position. It is not appropriate, under any circumstances, to promote yourself online for personal or financial gain
- You are entitled to hold and express political beliefs, but political conversations online can be tricky, especially where a link might be drawn, intentionally or not, between your politics and your job. Ask yourself if it is appropriate for you to be involved
- Don't let your passion take over. Something said in the heat of the moment online, might affect your ability to deploy, or limit future career options
- Requests for information from others – for example a blogger or an individual with a subscription account on a network – should be treated in the same way as a traditional media request and involve Defence Public Affairs (DPA). Even if an informal approach is made for information from someone you consider a friend, take it to DPA
- Talk to your colleagues about social media and the best way to approach it in your unit. If you are a social media whizz but your mates aren't, talk them through their privacy settings and help them stay safe too
- Remember once information is out there, you can't get it back. Your comment or opinion on someone else's post can go public – and viral – straight away

Case study

## What happens when you tag?



**Don't tag them #ProtectYourMates**

***When images are uploaded to the New Zealand Defence Force (NZDF) social media channels (unless the post is a specific story or congratulations about that person), personnel are not named in the imagery – protecting their identity.***

*However, often members of the NZDF are then tagged in the social media posts (specifically Facebook). There's banter, conversation and sometimes behaviour that is close to bullying.*

*In 2018, a female member of the New Zealand Defence Force was tagged by a colleague (and close friend) in the comments of a Facebook post that featured an image of her.*

*Shortly after the tag, this person was private messaged by some unwelcome Facebook users. They told her how beautiful she was and she was asked multiple questions about her job.*

*Not only did this tag identify the NZDF personnel, it also gave anyone with a Facebook account a way of contacting her.*

*This proved to be an uncomfortable experience for our NZDF personnel – and it was entirely avoidable.*

# What's on the web? 9

**When sharing content on social media, keep in mind that the Defence Public Affairs team is always looking for quality social media content.**

**You can email your content to socialmedia@nzdf.mil.nz or get in touch via other options if it's too big to send inside the NZDF system.**

***Below are a list of the social media platforms you may look to use in your personal life.***

### Facebook

Despite many people moving away from it, Facebook is still New Zealand's most popular social network (2018).

Facebook lets you share what's important to you instantly. You can be part of a community, instant message, video call, chat and message inside Facebook as well as post photos, comments and updates or play games.

***Tip:*** *Lock down your privacy settings so you know exactly who you're sharing with, what you're sharing and when. Disable location tags. Read the 'How to Keep Safe on Facebook' guide.*

### Facebook Messenger

This instant message app is owned and operated by Facebook. This app allows users to send messages and exchange photos, videos, stickers, audio and files, as well as react to other users' messages and interact with bots. The app also supports voice and video calling. Users don't require a Facebook account to have Facebook Messenger.

### Instagram

One of many photo-sharing networks which will automatically post to Twitter and Facebook. You can comment on photos and share them with others as well as getting artistic with filters and colours.

***Tip:*** *Disable GPS, disable location services, decide carefully if you want Instagram to automatically share to other networks. Read the 'How to Keep Safe on Instagram' guide.*

### Twitter

Twitter is the water-cooler of the web and currently the go-to global source of breaking news and information.

***Tip:*** *Every tweet is public and even if you opt for a protected account, a tweet may still become visible by someone else screenshotting it. Turn off geolocation, check settings, be mindful of what you share. Read the 'How to Keep Safe on Twitter' guide.*

### Skype

Free service allowing you to make video calls over the internet. Great for staying in touch and you can use it from your smartphone.

***Tip:*** *Check geolocation settings – turn off GPS.*

### Pinterest

A popular network that is essentially a visual online scrapbook. You can share your interests – anything from horticulture to architecture – and your stories with like-minded people.

***Tip:*** *Check settings – this network can also auto-share through to other platforms. Be careful who you make friends with as interests bring together strangers as friends.*

### Snapchat

A photo and video-sharing app. The photo or video is usually only available for a short time. This may seem like a great way to share content because it disappears but that's not completely true. Images/ videos can be screenshotted and can be seen again.

***Tip:*** *Turn off the location sharing feature 'snap map'. Read the 'How to Keep Safe on Snapchat' guide.*

### Spotify

One of many music apps. Make playlists, enjoy the music, as you work or in the company of friends.

***Tip:*** *When you log in with other accounts, the app will automatically post updates on your behalf – disable this ability in your settings.*

### YouTube

Video sharing website and search engine. Post video clips, find out how to do things, share moments with friends and family. Free to use, if you sign in to YouTube you are signed in across Google.

***Tip:*** *Check your settings, check your images for sensitive detail, and keep regulations in mind.*

### WhatsApp

A free cross-platform messaging and voice over ILP service owned by Facebook. It allows the sending of text messages and voice calls, as well as video calls, images and other media, documents and user location.

***Tip:*** *Check settings and understand that nothing is ever completely secure.*

**Stay social**

For more help on staying social—and staying safe—talk to the Digital Channels team in Defence Public Affairs at **socialmedia@nzdf.mil.nz**

10

# How to stay safe on social media guides

10.1

# 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.**

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

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.*

## 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

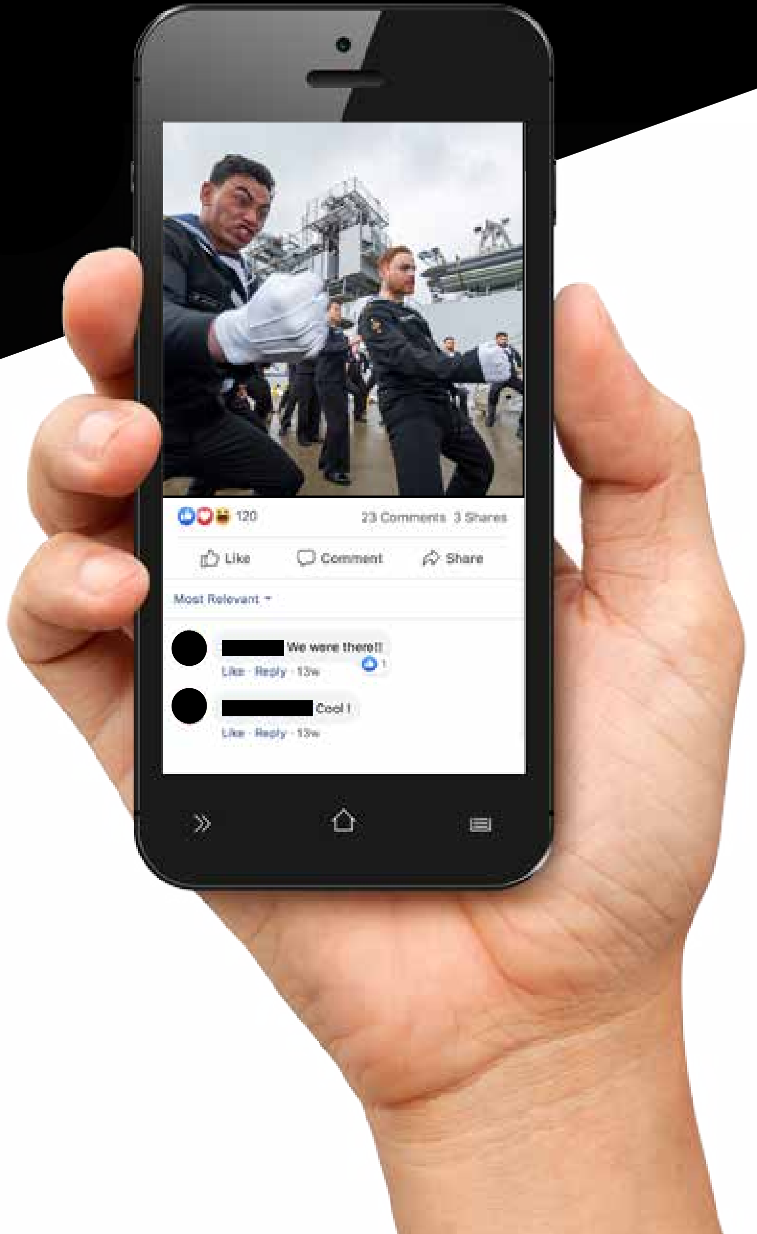
Facebook uses the location services on your phone or tablet to share more about who and where you are, both to your followers and their own advertisers. You should avoid adding location tags to your posts while at work (including exercises and operations).

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

**Don't tag them #ProtectYourMates**



120

23 Comments 3 Shares

Like Comment Share

Most Relevant

[redacted] We were there!!

Like · Reply · 13w

[redacted] Cool !

Like · Reply · 13w

10.2

## How to keep safe on Twitter

**Twitter can be an important tool for communicating messages to media and engaging with key leaders and influencers. Twitter is really only relevant for an international audience as only 21% of New Zealand's population use it.**

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

To ensure that your use of Twitter doesn't pose a risk to you, your family, your mates and your employer, we've got seven 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.*

### NZDF's seven safety tips for Twitter

**1. Online is for all time**

Even deleted content can linger on in cyberspace. Don't tweet anything you wouldn't be prepared to defend to your CO tomorrow (or in ten years time), and keep in mind that a poorly thought out tweet, retweet or like today might have implications for the security clearance you need for your next dream posting.

Any tweet should be thought of as being publically accessible. Even if it's a private tweet, once it's on someone else's screen, you have no control over it.

**2. Keep your privacy and security settings on lockdown**

As a member of the New Zealand Defence Force, it's recommended that you lock your profile down. Have you ever checked what the public can see on your profile? Making sure people can only see and read what you want them to is an important part of keeping yourself safe on social media. To check, go to 'Settings and Privacy' and look at your settings.

**3. Add two-factor authentication**

Like any username/password access, your user access can be hacked. It's important that 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 Twitter 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.

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

**4. 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 tweets and retweets – particularly on NZDF or Service Twitter Pages.

### 5. 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:

- Tap 'Settings and Privacy'
- Tap 'Password'
- Type your current password. Then type your new password and re-enter it one more time
- Tap 'Save Changes'

### 6. Choose your followers wisely

It's a fairly obvious, but don't allow people to follow you when you don't know them. Accepting them as a follower will allow them to view all your tweets and other information you allow them to see.

Also, be careful when accepting people who could be posing as someone else you're already friends with. Sadly, this does happen often. If this happens to you, let that friend know and report the fake account to Twitter.

### 7. Protect your location

To protect your location, avoid adding location tags to your tweets while at work (including exercises and operations).

To remove locations completely, you can turn off your location services. Go to 'Settings' > tap 'Privacy' > tap 'Location Services' > Scroll down and tap 'Twitter' > select 'Never'.

**Useful link**

Twitter Help Centre:
**https://help.twitter.com**

10.3

## How to keep safe on
# Instagram

**Instagram can be a fun communication tool for keeping in touch with family and friends, as well as showcasing quality images and video. As with any social media tool, these benefits come with some risks that you need to be mindful of as a member of the New Zealand Defence Force.**

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

To ensure that your use of Instagram 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.*

## NZDF’s six safety tips for Instagram

### 1. Online is for all time

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 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 account or chat, once it’s on someone else’s screen, you have no control over it.

### 2. Keep your privacy and security settings on lockdown

As a member of the New Zealand Defence Force, it’s recommended your Instagram account is set to private. This means only your approved followers will see your posts and stories. To set your posts to private from the Instagram app on iOS:

- Go to your profile by tapping 👤
- Tap ⚙ (iPhone) or ⋮ (Android) in the top right
- Tap ‘Account Privacy’ then tap to toggle Private Account on ✓

### 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.

If you’re logged out of your account and can’t remember your password, you can request to reset it.

To change your password:

- Go to your profile by tapping 👤
- Tap ⚙ (iOS) or ⋮ (Android) in the top right
- Scroll down and tap ‘Change Password’
- Enter your old password and then your new password
- Tap ‘Done’ or in the top right ✓

### 4. Tagging can be dangerous

Ensure that your privacy settings are set 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 videos, 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 Instagram pages.

### 5. Choose your followers wisely

If there’s someone who’s following you and you don’t like their content or their behaviour towards you, you can block or unfollow them (only if you have a private account).

When you block someone, that person won’t be able to find your profile, posts or story on Instagram. People aren’t notified when you block them.

### 6. Protect your location

Instagram 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 locations completely, you can turn off your location services. Go to ‘Settings’ > Tap ‘Privacy’ > Tap ‘Location Services’ > Scroll down and tap ‘Instagram’ > Select ‘Never’.

**Useful link**

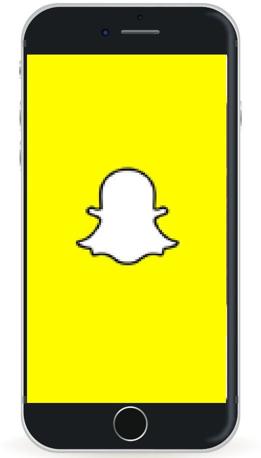
To learn more, visit the Instagram Help Centre at **help.instagram.com**

10.4

# How to keep safe on Snapchat

**Snapchat can be a fun way of keeping in touch with family and friends, as well as showcasing what you're up to right now. As with any social media tool, these benefits come with some risks that you need to be mindful of as a member of the New Zealand Defence Force.**

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



To ensure that your use of Snapchat 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.*

## NZDF's six safety tips for Snapchat

### 1. Online is for all time

Even deleted content or expiring content on services like Snapchat 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 set to expire, once it's on someone else's screen, you have no control over it.

### 2. Choose your followers wisely

It's fairly obvious, but don't allow people to follow you when you don't know them. Accepting them as a follower will allow them to see your content.

Unfortunately you also need to be careful when accepting people you know as followers. People have been known to set up fake accounts using real people's identities in order to make contact with their friends or family. If this happens to you, let your friend or family member know and report the fake account to Snapchat.

### 3. Block strangers who try to contact you

If you receive repeated attempts at contact from people you don't know, it's best to simply block them.

To block a user:

- Make sure you're on the user profile page
- Tap 'My friends'
- Tap a friend that you wish to block
- Tap 'Settings' at the top right hand corner
- Tap 'Block' and select a reason for blocking the person

### 4. Protect your location

It's best to not share your specific location, address and vehicle licence plates. While it can be tempting to add a snap with a geo-filter of your neighbourhood to a public story, it's safer to use filters that don't reveal your location.

To turn off location sharing:

- Go to 'Settings' > tap 'Snapchat' > tap 'Location'
- Switch it from 'While Using the App' to 'Never'

***Tip:*** *Try using the 'pen' option and censor out car licence plates if you really need to send out a snap that includes this information.*

### 5. 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.

### 6. Add two-factor authentication

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 Snapchat 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.

To set up a two-factor authentication:

- Tap 'Settings' at the top right corner of the screen
- Select 'Login verification'
- Click the green 'Continue' button
- Select 'SMS'
- Open the text message from Snapchat and type in the six-digit code into Snapchat
- Tap 'Continue'

**Some useful links**

- Snapchat's privacy policy. **www.snap.com/en-US/privacy/privacy-policy**
- Snapchat's 'Community Guidelines'. **https://support.snapchat.com/en-GB/a/guidelines**

# Social media glossary

## 11

**Algorithm**
The social media algorithm is a way of sorting through posts in a user feed. The intent of the algorithm is to provide the social media users with content they're most interested in.

**API**
An API (Application Programming Interface) allows one software programme or application to interact with another. For example, Tweetdeck and Hootsuite have APIs that work with social media platforms.

**AMA**
Short for 'ask me anything'.

**Analytics**
Data, and the patterns found in the data, often used to make marketing or advertising decisions.

**Avatar**
This is the image used to represent a person or an organisation. It is best to be consistent with your avatar so that it becomes instantly recognised across networks.

**Bitmoji**
Customised avatars that can be added to various platforms. You can also create an animated representation of yourself. It offers a variety of versions of the avatar in different situations that you can share with an app or smartphone keyboard.

**Bitly**
Bitly is the name of a free programme that can be used to shorten URLs (unique resource location), known to most of us as the web address bar. Short URLs are used across the social networks, but particularly in Twitter where the character count is small (280). Another shortening service is available free at http://goo.gl.com and, like http://bit.ly.com, provides data on traffic and shares.

**Block**
A feature that allows you to prevent a user from engaging, seeing your content, tagging you in photos etc.

**Blog**
Originally weblog, but shortened many years ago to 'blog' by a journalist from the UK Guardian newspaper, a blog is a self-publishing system, maintained by an individual, company or other organisation on a regular basis. It can be used to create a micro-site in an emergency or for a particular event. Blogs are used by organisations as their primary news publishing channel.

**Blogger (someone who blogs)**
Regular bloggers are recognised as media in many places – David Farrar of kiwiblog.co.nz being one example. Blogger is also the name of a free platform for bloggers run by Google at blogger.com.

**Cloud**
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over the Internet. Cloud computing entrusts remote services with a user's data, software and computation and has become increasingly popular as it can substantially reduce costs.

**Comment**
Any response to a post or status notification, either on a blog, a Facebook post or other chat/comment enabled platform. Comments need to be monitored and answered. They are also a credible means of measuring sentiment.

**Creative Commons**
A non-profit organisation making it easier to share content with others. It is a means of working within existing copyright laws, granting licenses for use in particular circumstances: www.creativecommons.org.nz.

**Crowdsourcing**
An important development online, originating around ten years ago, originally on blogging sites. A means to collect the creative wisdom of the crowd by asking questions, problem solving and sharing information on the web. Very popular among journalists and authors as well as the science community.

**DM or Direct Message**
A private message sent on a social media channel.

**Dropbox**
A service that lets you bring your photos, videos and words together and share them easily with others: www.dropbox.com.

**Emoji**
A small icon used to represent an emotion, symbol or object.

**Engagement**
Talking to, messaging, or otherwise interacting with other people on social networks. It encompasses many types of actions, including commenting and reactions.

**Evernote**

Similar to Dropbox, Evernote helps you share your materials across devices, pushing notes, documents etc., from phone to laptop to tablet or to cloud.

**Facebook**
Social networking website where individuals can create a profile, keep in touch with friends and family, play games, follow other organisations and stay up-to-date with news and information generated by those organisations.

**Facebook Group**
A feature within Facebook where users can build a community and communicate and share content with a select group of people.

**Facebook Live**
A feature within Facebook that allows you to stream live video to your family, friends and followers.

**Facebook Messenger**
An instant message service owned by Facebook. Used for personal use but also business.

**Filter**
A photographic effect that can be applied to images/videos before publishing them.

**Flashmob**
A big group of people who come together quickly in one place to perform, demonstrate or highlight an issue.
Most flashmobs are benign, but protest flashmobs are on the rise.

**Follow**
An action taken by network users to stay up-to-date with somebody else. On Twitter, you 'follow' other people and they can 'follow' you, which means that they have specifically chosen to receive your information.

**GIF**
An acronym for Graphics Interchange Format, which refers to a file format that supports both static and animated images.

**Handle**
Your online identity and also sometimes referred to as username e.g. @NZDefenceForce.

**Hashtag**
A hashtag is used to group conversations and subjects on various different platforms, creating a category that people can follow or search for. A social media hashtag in use would look like this: #socialmedia.

**Hootsuite**
An application that works with all social platforms. It allows the user to monitor, engage and report on their social media activity.

**Insights**
The metrics used by Facebook to determine trends, user growth, demographics etc.

**Instagram**
Also known as IG or Insta. It's a free online photo and video-sharing app owned by Facebook. The social network allows for the addition of several filters, editing and sharing options. The app also allows video upload and storytelling with the story feature.

**Instant messaging**
Real time direct messaging between people – commonly found in Facebook, Google, Twitter, Skype.

**Like**
An action taken on Facebook to indicate approval. Replaces or is used in addition to writing a comment. 'Likes' are used as a metric.

**LinkedIn**
Social networking for business.

**Livestream**
Allows people to view and broadcast video using camera and computer via internet or mobile phone.

**Lurker**
Someone who trawls the internet, follows people and content but doesn't contribute.

**Mashup**
A mashup draws content from a variety of sources and pushes it together to create new work.

**Meme**
Memes are a way of expressing a culturally-relevant idea. A meme is an image or video that represents the thoughts and feelings of a specific audience, usually captioned directly on the image or video.

**Mention**
The act of tagging another user's handle or account name in a social media message or caption. This then triggers a notification for that user.

**News reader**
Allows people to aggregate news and information from many sources using RSS or Atom Feeds (XML). Google Reader is an example.

**QR code**
QR (Quick Response) codes are two dimensional code that contains information readable by phone cameras. Normally a black and white pattern, it can be customised and coloured.

**Reactions**
Most commonly used on Facebook but now also LinkedIn, reactions are used to express ourselves and translate our emotions in a digital format. Reactions can include love, ha-ha, like, wow, sad and angry.

**Reach**
The metric that determines the maximum potential audience for any given post. The number is determined by complex calculations that include followers, shares and impressions as well as other metrics.

**Retweet**
A tweet that is re-shared to that user's followers. A user can republish as is or with a comment.

**RSS**
Originally stood for Rich Site Summary, known widely now as Really Simple Syndication. The code behind RSS is the language that lets the web move. An RSS document includes full text, summarised text, author, dates and other metadata.

**Sentiment**
Metric within social media for determining the position of a community towards an organisation, issue or brand.

**Selfie**
A self-portrait photograph taken with a smartphone.

**Slideshare**
Online network for sharing presentations and documents.

**Skype**
Free VoiP software (voice over internet protocol) that allows users to make free video and voice calls. Extra subscription allows video conferencing. Mobile Skype is widely used.

**Snapchat**
A photo and video-sharing app. The photo or video is usually only available for a short time.

**Social media**
Collective description for internet based communication channels, tools and technologies.

**Social media monitoring**
Listening and responding to conversations and mentions of your organisation.

**TweetDeck**
Similar application to Hootsuite, connecting social networks. Tweetdeck is used around the world to monitor Twitter.

**Tweet**
A twitter message. These have a character limit (280) and can include various forms of media.

**Twitter**
Microblogging platform where people exchange real-time updates with character limits (280). All messages appear on the public timeline unless tweets have been protected. Twitter is the main news breaker across the world.

**Tumblr**
Microblogging platform but more visually based.

**Verified**
An account whose owner has proven their identity with the social media platform providers.

**Vimeo**
Video sharing platform.

**Wechat**
A Chinese multi-purpose messaging, social media, and mobile payment app.

**Wordpress**
World's most popular free blogging platform – best for creating microsites.

**YouTube**
Largest video sharing site in the world.

# How to find us on Social Media

# 12

## Facebook

@NZDefenceForce
@NZNavy
@NZArmy
@NZAirForce

**Join the conversation on our Facebook groups:**

NZDF Community Alerts
NZDF Sport
NZDF Community
Royal New Zealand Navy Community
New Zealand Army Community
Royal New Zealand Air Force Community

## Twitter

@NZDefenceForce
@NZNavy
@NZArmy
@NZAirForce

## Instagram

@NZDefenceForce

## YouTube

Check out our YouTube channel. Videos about the work we do and the capabilities we have.

## LinkedIn

Follow us on LinkedIn.
Find out about NZDF's role as an employer and read stories about our staff and partners.

**Want to post on our NZDF social media sites?**

Get in touch with the team at **socialmedia@nzdf.mil.nz**

Visit **NZDF.mil.nz** for the latest social media channels list.

A FORCE FOR
NEW ZEALAND