Personal Social Media Guide

Practical advice for ADF, APS and contracted personnel

As at May 2022

(Note document is not controlled if printed)

Contents

Using this Guide

The Personal Social Media Guide is designed for Australian Defence Force (ADF) and Australian Public Service (APS) and contracted personnel to provide advice on using social media personally.

This guide should be read in conjunction with Chapter 7 in the Defence Media and Communication Guide.

The use of social media has increased exponentially and continues to be embraced. This has led to a blurring of lines between professional and private online activity which can present privacy and security issues.

Defence personnel are allowed to use social media personally, but must ensure their comments, photos and online associations do not compromise operational or personal security.

Any feedback on the *Personal Social Media Guide* is to be sent to the Social Media Hub at s47E(d) @defence.gov.au.

Social media policy

Defence recognises and accepts reasonable use of social media that doesn't interfere with effective completion of work or contravene the Defence Social Media Policy.

There are consequences for personnel using social media inappropriately, including possible disciplinary action or criminal prosecution. Failure to comply with Defence policy could constitute an offence against provisions of the *Australian Defence Force Discipline Act 1992*, the *Public Service Act 1999* and/or amount to a breach of the *Australian Public Service Code of Conduct*.

Review the following Defence and Commonwealth policies:

- Defence Media and Communication Policy is the policy for the use of social media by Defence personnel.
- Defence Media and Communication Guide. This Guide applies to all Defence personnel and must be adhered to in accordance with the Defence Media and Communication Policy.
- Australian Public Service Commission Code of Conduct is the policy for the ethical standards and values APS employees should uphold and is set out in section 13 of the *Public Service Act 1999.*
- Australian Public Service Commission Code of Conduct in Practice is the current guidance on making public comment and participating online (social media).
- Defence Force Discipline Act 1982 is an act relating to the discipline of the Defence Force and for related purposes.
- Defence Security Manual is the publication which implements in Defence the minimum standards of the Government Protective Security Policy Framework (PSPF) and Government Information and Security Manual (ISM).
- Privacy Act 1988 is an Act to make provision to protect the privacy of individuals and for related purposes.
- Work Health and Safety Act 2011 is an Act relating to work health and safety, and for related purposes.

Social media usage

Principles

Publishing online is public comment, and use of digital channels in a private capacity must be consistent with the values and strategic messages of Defence. It is essential that you do not post any content or engage in any activity that could be seen to damage the reputation of Defence.

- ❏ What would your Chain of Command, the Secretary, the Chief of the Defence Force, and/or adversaries think of your social media activity?
- ❏ Do not criticise the work or administration of the Government, Department, Group or Service. You must professionally and impartially serve the government of the day
- ❏ Do not discuss any internal Defence material including forecasting, announcing or promoting Defence activities that have not been disclosed previously in the public domain
- ❏ Respect privacy, be respectful, be polite and don't post any defamatory, vulgar, obscene, abusive, profane, threatening, racially or ethnically hateful or otherwise offensive or illegal content
- ❏ Do not claim or appear to represent Defence as an official spokesperson.
- ❏ You are accountable for your actions online. Do not like, join, share, engage or remain a member of a page, account, group, forum, site or discussion that is involved in or promotes behaviour that is exploitative, objectifying or derogatory or in any other way breaches any relevant legislation or Defence policies.

Public comment

Personal social media accounts must not use any Defence branding (including Defence logos, emblems, badges, symbols, iconography etc.); official title; rank; profile photo in uniform or other clothing with Defence branding; position/employment category; role; or organisational grouping connected to or representing Defence.

The exception is LinkedIn, where personnel are permitted to reflect their role within Defence, provided no operational or classified information is contained in the account. Access LinkedIn via the official website or mobile application and consider using a different email address for LinkedIn access from the email address used for personal communication.

If an account appears to be representing Defence, and is administered by Defence personnel, all content and activity will be deemed departmental public comment and that individual will be

accountable for compliance with the requirements of the Defence Media and Communication Policy and other relevant Defence policies.

Maintaining security for Defence operations

If you have any doubt regarding operational security, you must seek appropriate guidance and clarification from your Chain of Command or Supervisor prior to making material public.

Staying safe online

Privacy and security settings exist for a reason. You need to learn about and use the privacy and security settings on social networks. They will help you control who sees what you post and manage your online experience in a positive way.

It is part of your job to be wary about how much information you post or make available online. Remember, what you post online stays online forever so be cautious about the personal information you provide on social media.

No information that breaches security or adversely affects the safety and wellbeing of Defence personnel and their families, or damages Defence's reputation and international relationships can be published.

In the context of security clearance, AGSVA may take into account behaviour on social media.

For general tips on staying safe online, visit https://www.staysmartonline.gov.au/

Geotagging

Geotagging adds geographical data to various media including photographs or video, websites, SMS messages, providing details of exactly where the media was taken. Most photos taken on a smartphone with GPS capabilities are usually geotagged automatically unless you have turned off the setting.

For security purposes, it is recommend that Defence personnel turn off geotagging.

Securing your account

Digital security is more important than ever.

It is important you keep your social media account/s secure. Use this checklist as your guide:

- ❏ Your password should include a mixture of numbers, symbols, and capital and lowercase letters.
- ❏ Change your password at least once every three months and when possible, use two-factor authentication.
- ❏ Use separate passwords for every account. At a minimum, separate your official and personal accounts and make sure your critical accounts have strong passwords.
- ❏ Remember to log out whenever an account isn't in use.
- ❏ Be aware that criminal and/or terrorist organisations and foreign intelligence services actively seek information about Defence capabilities which may potentially harm Defence personnel, information and/or interests. Some people online may disguise their real identity in order to elicit personal or operational information from Defence personnel or their families and friends.
- ❏ No information should be given out in response to requests for information through digital channels without appropriate clearance. Requests for information are to be treated like a media enquiry and forwarded to Media Team on s47E(d)@defence.gov.au.
- ❏ The Defence Secret and Restricted Networks System User Acceptable Usage Standard Operating Procedures provides guidance about online security considerations when using online applications, including social media, on the DPN and DSN, which also apply to other Defence ICT assets.

Setting up your personal social media account/s

Profile Picture

Your account picture is one of the first things that people will see.

Do not use an account picture with your service uniform for any personal accounts.

As your Profile Picture will always be public, ensure you do not have a passport style profile picture with your face forward facing, as these can be used to steal your identity. Cover a portion of your face, or use an avatar to protect your identity.

Connecting

At your discretion, follow/friend/connect with stakeholders who are of influence in your environment. However you should not follow groups or stakeholders who may post inappropriate content or that may pose a security risk.

Posting, commenting, liking and sharing

Social media is built around participation and engagement with your followers/friends/connections.

Keep in mind that when using any social media site you represent the values of yourself and your workplace. If you are commenting as an expert on a topic you should ensure it is clear that the views are personal and not the views of your employer.

All conversation and activity should be carefully moderated. Do not engage in:

- ❑ Ill -natured debates (arguments)
- ❑ Criticism of others
- ❑ Not safe for work content
- ❑ Internet trolls
- ❑ Discussion of religion or politics
- ❑ Disclosing internal Defence, confidential or classified information
- ❑ Harassment of an individual both publicly and privately on the site

Managing your account

Community Standards

Each social media platform has *Community Standards* that provide guidance to users on what is and is not allowed on their platform. Content that breaches the community standards may be removed, and if frequent breaches occur, the account may be closed.

The main platforms used in Australia are listed here:

- ❏ Facebook – https://www.facebook.com/communitystandards
- ❏ Twitter - https://help.twitter.com/en/rules-and-policies#twitter-rules
- ❏ Instagram - https://help.instagram.com
- ❏ LinkedIn - https://www.linkedin.com/legal/user-agreement

Moderation

Moderation is the manual or automatic process for assessing and removing social media content (including images, comments/replies etc.) that is considered extreme and offensive by the contributing community. You should moderate your own accounts to ensure that comments/replies are in line with the relevant platform's community standards.

It is important you moderate:

- ❏ profanities (at an age-appropriate level for the audience)
- ❏ abuse and personal attacks
- ❏ hate and discrimination
- ❏ obscenity
- ❏ personally identifying information
- ❏ security breaches
- ❏ breaches of the general code of conduct
- ❏ incorrect information.

While some social media platforms like Facebook automatically moderate for basic breaches, such as the use of profanities, some of the followers of your accounts may not be aware of what behaviour is acceptable and what is not. You may also block or delete users if you consider they have breached the social media networks' fair use policy.

What to do if you are being harassed or bullied online?

Protect yourself, seek support and report

If you are harassed or bullied online you should take action as quickly as possible. Unfortunately there are incidents daily across social media. We recommend to take the following steps:

- ❑ Protect yourself
- ❑ Seek support
- ❑ Report

It is recommended that you first protect yourself and your family. Immediately review your privacy settings and un-tag yourself from any posts where the harassment or bullying has occurred.

Secondly, seek support. Defence provides counselling services, you can approach your Chain of Command or see your Services Chaplain, or contact one of the organisations listed below.

Third, report the incident to your Chain of Command, the Defence Social Media Hub on s47E(d) @defence.gov.au, and report through the relevant social media platform.

Protect yourself

- Review your privacy and security settings
- Un-tag yourself from any posts
- Advise your family and friends not to tag you in posts, and set the function for you to approve any future tags

Seek support

- Talk to your Chain of Command.
- Call the Defence All Hours Support Line (ASL), a confidential telephone service for ADF members and their families. ASL is available 24 hours a day, 7 days a week on s47E(d)
- APS staff can utilise the Defence Employee Assistance Program (EAP). EAP is available 24 hours a day, 7 days a week on s47E(d)
- Or seek support via Lifeline or 1800RESPECT.

Report

- The offending post to your Chain of Command. Take a screen shot of the post and any offending comments.
- If the post breaches Defence policy, contact the Defence Social Media Hub advising of the issue along with a screen shot/s.
- If the post breaches the platform community standards, report it through the platform's help centre. Keep a record of your report.

Additional information if you are being bullied or harassed online in connection to your employment with Defence.

Unacceptable behaviour can occur at any place and in any environment, whether in Australia or overseas, where the behaviour may be connected to Defence. This includes social media and virtual platforms. Personnel must comply with the Defence Values and Behaviours where their actions are connected to their employment with Defence.

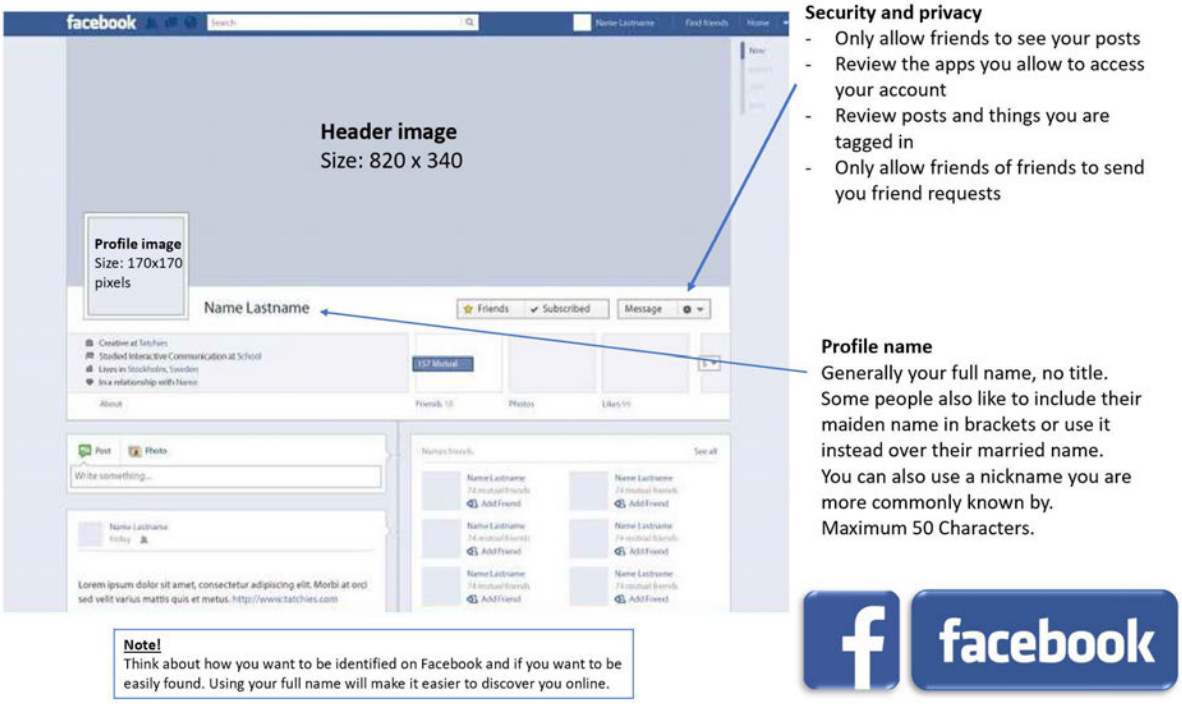
If you experience behaviour online that can reasonably be interpreted as unacceptable behaviour and there may be a connection to your employment, further advice, reporting and support options are detailed in the Complaints and Alternative Resolutions Manual Chapter 3 – Responding to Unacceptable Behaviour.

Quick reference guide - Privacy Settings

Recommended Facebook Privacy settings:

1. To adjust privacy settings click the ▼ at the top right of Facebook and select **settings.**
2. Click **Security and login** on the left column
3. Make sure you have a secure password and it is changed often.
4. Next, click on the ? icon next to the arrow on the top right corner and click on **Privacy check up**
5. Go through the prompts and set everything to only let **friends** view your posts, you can also create a list to only let certain friends see certain posts i.e. only allow family members to see the images you post from your birthday.
6. Next click on the ▼ at the top right of Facebook and select **Privacy** from the menu on the left column.
7. You can go through the menu that appears and set each setting to **friends** only.
8. Select **no** for appearing in search engine results.
9. You can also set up your account so that you have to approve every post you are tagged in i.e. Facebook status updates and pictures posted by friends.
10. On the left column, select apps.
11. You can adjust the settings for each individual app, you can click on each one individually. Deselect all options, some apps will not allow you to untick all the options so you should consider removing the app if it is not necessary.

Setting up your personal Facebook account



Recommended Twitter privacy settings:

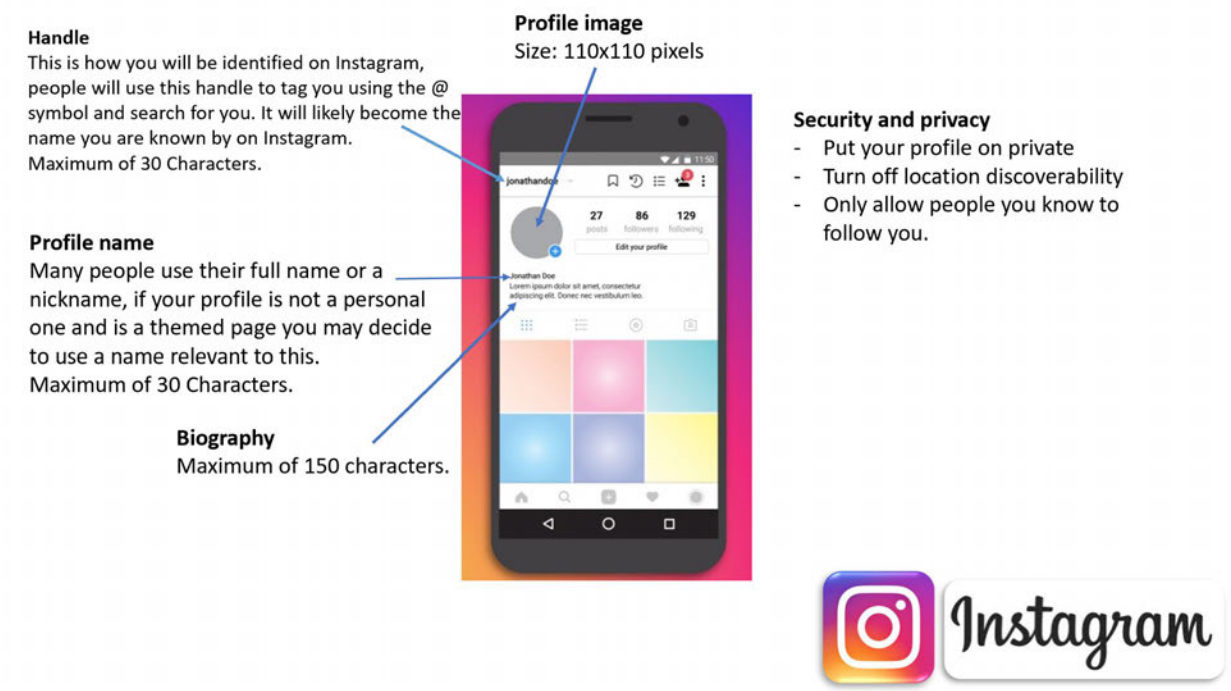
1. Ensure you use a secure password and it is changed often
2. When logged in, click the account icon on the top right of the screen, select **settings and privacy**
3. Click on the **password** tab, enter you current password and new password and save changes.
4. Your account should require verification when changing your password, particularly if you have multiple users logging in from different devices. Go to **account settings**
5. Under the **security** section, check the box next to **require personal information to reset my password.**
6. You will be required to enter your account email address or phone number.
7. You should also have two-step verification in the top menu click on the account icon and click **settings and privacy**
8. Click on your **account settings** and select **setup** login verification
9. Read the overview instructions and click start
10. Enter your password and click **verify**
11. Click **send code** to add your phone number.
12. Enter the verification code and click **submit**
13. Click **get a backup code** to view a code generated by twitter. It is best to store this code in a safe place as it will help you access your account if you lose your phone or change your phone number.

Setting up your personal Twitter account

Recommended privacy settings on Instagram:

1. Ensure you have a secure password and it is changed often, select the three lines and select **settings** at the bottom of the menu that appears.
2. Select **password** and save it once it is changed.
3. Don't allow access to third party applications other than your post scheduling tool.
4. You should have two-factor authentication set up particularly if there are multiple persons accessing the account.
5. Go to **settings**, scroll down to two-factor authentication and switch on **require a security code**

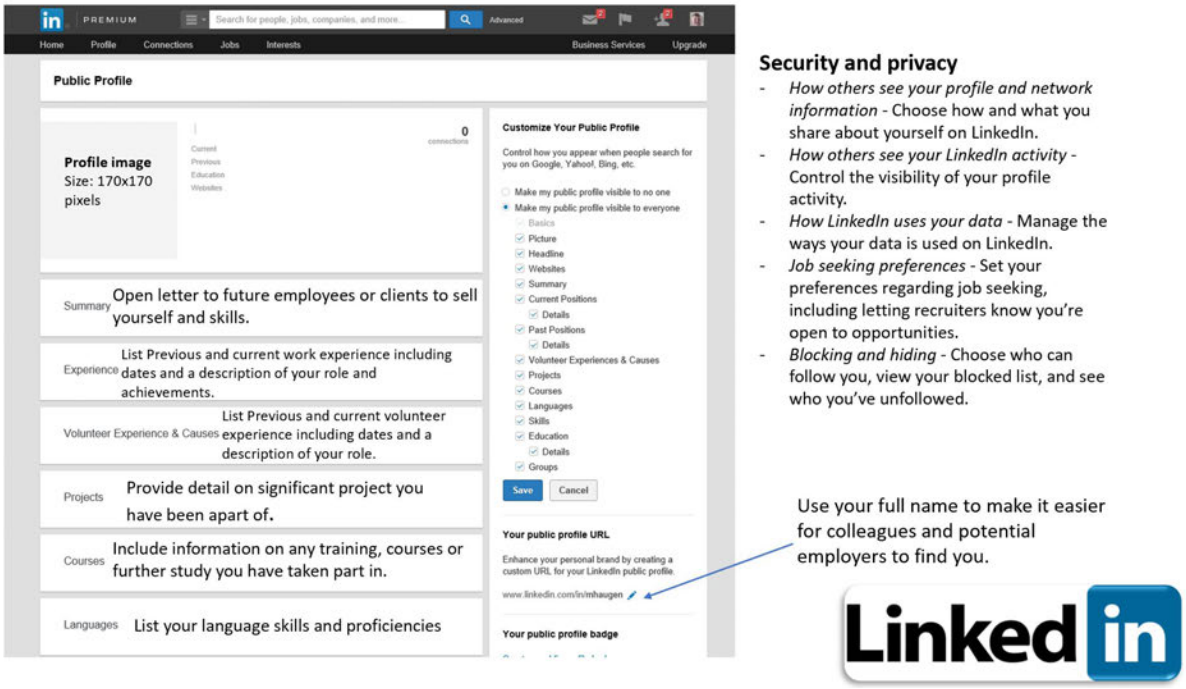
Setting up your personal Instagram account



Recommended privacy settings for LinkedIn:

1. Ensure you have a secure password that is changed often
2. Click on the **me** icon at the top of the homepage
3. Select **settings and privacy**
4. Under the **login and security** section of the account tab, click **change** next to **change password.**
5. Select the checkbox to **require all devices to sign in with the new password**
6. Turn on two-factor authentication
7. Click the **me** icon at the top of your LinkedIn homepage
8. Select **settings and privacy**
9. Under **login and security** section of the **Account** tab, click **Change** next to **two-step verification.**
10. Click **Turn on** to change the status of the two-step verification
11. Once you receive the code set to your phone, enter it into the box on the device you are signing in on
12. Click **verify**

Setting up your personal LinkedIn account



LinkedIn profile image and connections

If you choose to wear your service uniform in your account picture ensure that you have the correct uniform on. It should be a professional headshot or your official portrait and not an

image taken while on the job. Wearing your uniform in your account image makes you identifiable as Defence or ADF personnel to the public.

It is important to build your network in an intelligent, meaningful and strategic manner. Connect with people that work in the same field as you or that you share mutual interests or mutual connections with.

Appropriate LinkedIn behaviour:

1. Don’t post inappropriate content
2. Don’t send spam or unsolicited promotional messages
3. Don’t share classified or confidential information
4. Don’t Share political or religious views. Keep conversation and interactions professional
5. Don’t post memes
6. Don’t post misleading updates
7. Don’t argue or start arguments
8. Don’t use LinkedIn as a dating website.

Frequently asked questions

What type of content should I share?

Be proud of your association with Defence and be free to share cleared content appropriately for organisational reputation benefit. You can share Defence or Services content to your personal platform but ensure if retweeting or sharing with your own comments it aligns with Defence values.

Who should I follow?

At your discretion, follow/friend/connect with stakeholders who are of influence in your environment. However, you should not follow groups or stakeholders who may post inappropriate content or content that may pose a security risk.

Is there anyone I should not connect with?

Defence does not recommend to friend/connect with people who are unknown to you on your personal social media account. Remember that as an employee of Defence you are potentially a target for adversaries.

Is there anything I should do before going on deployment?

For any private social media account, we recommend adding a Legacy Contact if available on that platform. A legacy contact can look after your account if it is memorialised.

Your legacy contact can:

1. Write a pinned post for your profile (example: to share a final message on your behalf or provide information about a memorial service)
2. Update your profile picture and cover photo.
3. Request the removal of your account
4. Download a copy of what you've shared on the account.

Check the relevant platform's Help Centre for more information.

The issue I have is not covered in this guide. What do I do?

Refer to the relevant platform's Help Centre for further advice.

Australian Government
Defence

Social Media
for Personal Use

THINK BEFORE POSTING
Consider who will be seeing your post and what your message implies

KEEP OUR DEFENCE VALUES FRONT OF MIND
Consider if your post will damage Defence and/or your reputation and/or endanger your professional and personal life

BE CULTURALLY AWARE
Consider if your post will offend any group of people

DO NOT COMPROMISE SAFETY OF YOURSELF AND YOUR COLLEAGUES
Avoid posting images or videos that could potentionally allow our adversaries to gain classified information

Australian Government
Defence

A Quick Social Media Guide for Defence Personnel Working Overseas

Social media is used to understand, inform, educate, engage and influence our target audiences, as well as to amplify messages in a broader and more contemporary way. Your role overseas is one of a Brand Ambassador. You should promote the work of the overseas Post and Defence in the host nation and back in Australia, ensuring communication is aligned to key messages.

If you're managing an official account:

READ THE POLICY & ACCOMPANYING GUIDE
The Defence Media and Communication Policy and Guide must be adhered to and will help meet expected outcomes.

KNOW YOUR AUDIENCE
Understand their way of consuming information—each region will have a social media platform that is used more prolifically. For example, Facebook is used more than any other platform in Fiji, while in South Korea, Instagram is used more than Facebook. When you arrive in your overseas location, you will need to understand what social media platform is dominant—liaise with the DFAT public diplomacy team at Post for more information, guidance and clearance processes.

USE CLEARED OFFICIAL IMAGERY & OPTIMISE CONTENT
Each DFAT overseas Post will have one or more social media profiles. You should understand their content planning for the profiles and ensure that events, visits and other key Defence communication plans are built into their approach. Only cleared imagery should be published on official accounts. Remember to optimise your copy by using the relevant hashtags and account tags.

OFFICIAL DEFENCE ORGANISATIONAL ACCOUNTS
Accounts like ADF in PNG, ADF in Malaysia and IKAHAN have been established through an official process. When publishing to these accounts, consider if your content will offend any group of people. Remember that all new Defence social media accounts must follow a formal application process.

MAKE USE OF THE RESOURCES AVAILABLE
The Social Media Playbook should be used in conjunction with the policy. Visit the Defence Social Media Intranet page for up-to-date information.

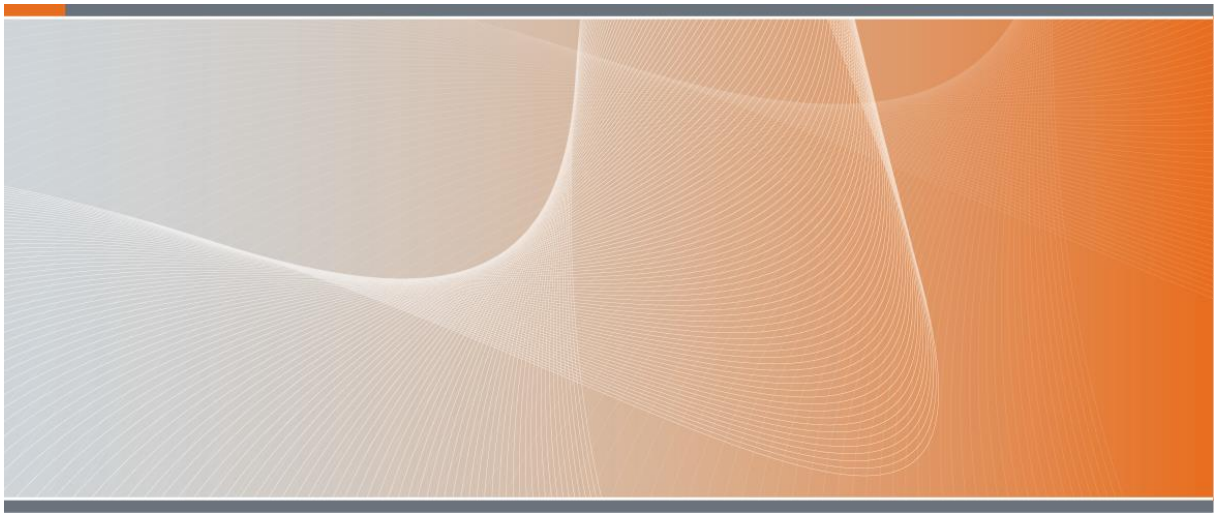
If you're utilising social media for personal use:

THINK BEFORE POSTING
Consider who will be seeing your post and what your message implies.

BE AWARE, DO NOT COMPROMISE SAFETY OF YOURSELF, YOUR FAMILY AND YOUR COLLEAGUES
Adversaries could gain classified information. Refrain from capturing imagery/video on your personal device for publishing on personal social media accounts.

Remember, there could be foreign Defence members with protected identities that should not be photographed. Consider if your content will damage Defence and/or your reputation and/or endanger your professional and personal life.

DEFENCE MEDIA AND COMMUNICATION GUIDE



s22

12 May 2022

Version 1.1 (issued 16 May 2022)

CHAPTER 7 – SOCIAL MEDIA (UNOFFICIAL)

7.1 Social media refers to websites and applications that enable users to create and share content, or to participate in virtual communities and networks. Social media includes, but is not limited to:

a. social media networking sites (e.g. Facebook, Twitter, LinkedIn, SnapChat etc.);

b. social review sites (e.g. Yelp, Tripadvisor, Goodreads, Google Reviews etc.);

c. image sharing sites (e.g. Instagram, Flickr, Pinterest etc.);

d. video hosting and live streaming sites (e.g. YouTube, TikTok, Zoom, Skype etc.);

e. community blogs (e.g. WordPress, Tumblr, Blogger etc.);

f. discussion sites and professional military education websites (e.g. Whirlpool, Quora, Reddit, The Cove, Forge etc.);

g. messenger sites (e.g. Messenger, Signal, WhatsApp etc.);

h. collaborative sites (e.g. Wikipedia etc.); and

i. dating sites (e.g. Tinder, RSVP, Bumble etc.).

7.2 An unofficial social media account is one operated by Defence personnel in a personal or private capacity for non-Defence related positions, organisations and activities, not associated with their service or employment in Defence.

a. For policy on the personal use of Defence's information and communications technology resources, refer to the Information and Communications Technology Manual.

7.3 Defence personnel can use social media in an unofficial capacity. This must be balanced with security and professional obligations as Defence personnel, where online behaviour can pose a risk to national security, and reflect on Defence as a whole. This ultimately may harm Defence's personnel, information or national interests, as well as impacting on organisational reputation and the level of confidence Defence receives from the Australian community and the Government. In some cases, responsibilities extend into Defence personnel's private lives and limit their ability to participate fully in public discussions, including on social media.

7.4 Unofficial social media accounts of Defence personnel must not use any Defence branding (including Defence logos, emblems, badges, symbols, iconography etc.); official title; rank; profile photo in uniform or other clothing with Defence branding; position/employment category; role; or organisational grouping connected to or representing Defence.

a. Defence personnel using **LinkedIn** must:

i. comply with the security considerations at paragraphs 7.11-7.13 and carefully consider the type and amount of information they post, including technical expertise;

ii. not use their rank, profile photo in uniform or other clothing with Defence branding, detailed information about their current or previous roles in Defence, or any operational, classified or sensitive information;

iii. apply the highest privacy and security settings available;

iv. only access LinkedIn via the official website or mobile application; and

v. consider using a different email address for LinkedIn access from the email address used for personal communication.

7.5 Defence personnel submitting content to internal or external professional military education parties (such as The Cove, Forge, The Runway etc.) must do so in accordance with Chapter 3 – Releasing Official Content or Making Public Comment on Behalf of Defence.

CONDUCT WHEN USING UNOFFICIAL SOCIAL MEDIA ACCOUNTS

7.6 Posts, comments, direct messages, likes, reactions, shares and similar activity on social media from people identified or identifiable as Defence personnel constitute public comment and are subject to the policies, values and legislation governing Defence. Failure to comply with Defence policy could constitute an offence against provisions of the *Defence Force Discipline Act 1982*, the *Public Service Act 1999* and/or amount to a breach of the *Australian Public Service Code of Conduct*.

a. The policies, values and legislation governing Defence apply even if material is posted anonymously or using a pseudonym and Defence employees should be mindful that their identity or employment may be revealed.

b. Joining, following or liking someone else's content could be perceived as endorsement of the content. Defence personnel should apply the considerations of paragraph 7.7 when joining, following or liking another person's content.

c. Being tagged in certain posts may imply an association. Where possible, Defence personnel must untag themselves from posts that do not comply with their responsibilities as Defence personnel.

d. Defence personnel are permitted to follow Members of Parliament across the political spectrum in the interests of staying well informed or because they support a particular party. Any engagement with such posts must be in accordance with paragraph 7.6.a.

e. Defence personnel should review their online footprint periodically, such as when joining Defence, changing roles or on promotion.

Historical posts should be considered in the context of all the risk factors and removed where appropriate.

7.7 Defence personnel using unofficial social media accounts must:

a. exercise discretion and judgement and protect classified and private information, operational security, our international relationships and the safety of Defence personnel and their families;

b. do so in a professional, impartial and apolitical manner;

c. behave with respect and courtesy;

d. ensure that personal comments added to official content released by Defence aligns with Defence Values and Behaviours;

e. be aware that what you post can affect your reputation, as well as that of the Government, ministers and Defence; and

f. be aware that content posted on social media is available immediately to a wide audience, effectively endures without limit, may be copied repeatedly, screen captured, may be seen by people who it was not intended for or used for a purpose for which it was not intended, or taken out of context.

7.8 Defence personnel using unofficial social media accounts must not:

a. release operational, classified or sensitive information, including but not limited to, details about operational incidents, missions, security procedures, locations and times of deployments, damaged equipment and assets, personal documents (such as wills, powers of attorney, deployment information etc.), and issues regarding morale or personnel;

b. release information about the injury, wounding or death of a Defence employee before the next of kin is notified and the information is publicly released by Defence;

c. criticise or question the role, work, policy or administration of the Government, Defence, or Defence Group or Service;

d. forecast, announce or promote Defence activities that have not been disclosed previously in the public domain;

e. claim or appear to represent Defence as an official spokesperson (such as, but not limited to, using Defence branding, including Defence logos, emblems, badges, symbols and iconography (see Chapter 9 – Defence Branding); official title; rank; position/employment category; role; profile photo in uniform etc.);

f. use imagery of Defence activities that have not been cleared for public release or represent Defence negatively in the public domain;

g. post any defamatory, discriminatory, vulgar, obscene, abusive, profane, threatening, racially or ethnically hateful, otherwise not aligned with Defence Values and Behaviours, or illegal information or material;

h. join, submit content to or remain a member of a group, forum, site or discussion that is involved in or promotes behaviour that is exploitative, objectifying or derogatory, goes against Defence Values and Behaviours or in any other way breaches any relevant legislation or Defence policies; or

i. use media where the copyright is owned by anyone else without authorisation or permission.

CLEARANCE TO USE IMAGERY/AUDIO ON UNOFFICIAL SOCIAL MEDIA ACCOUNTS

7.9 Defence personnel can post imagery (photographs or videos) of themselves in uniform provided they have appropriate clearance by their chain-of-command. Prior to posting, imagery must be closely reviewed to ensure no operational, classified, sensitive or personal information is released (such as troop locations, equipment, tactical unit details, numbers of personnel etc.).

a. Images of Defence personnel in uniform must not be used as profile pictures on any unofficial social media accounts. The only exception to this is ForceNet, where the use of a profile picture in uniform is permitted.

b. Defence personnel are permitted to post images that have been published on the Defence Image Gallery (in accordance with paragraph 7.6.a) or videos that have been published on the Defence Australia YouTube channel.

c. Images, videos or audio taken by Defence personnel on duty belong to Defence and must be cleared by the member's chain-of-command prior to release to ensure no operational, classified, sensitive or personal information is released. For further information regarding copyright of imagery or audio, refer to paragraphs 8.11-8.23 in Chapter 8 – Digital Media.

7.10 Defence imagery and audio must not be used for political purposes in a way contrary to Defence's apolitical standing. Defence personnel engaging in political activities must comply with imagery and audio requirements in accordance with paragraph 8.19 in Chapter 8 – Digital Media.

SECURITY OF UNOFFICIAL SOCIAL MEDIA ACCOUNTS

7.11 Defence personnel need to exercise caution with respect to their online presence and be aware that criminal and terrorist organisations, ideologically motivated groups, foreign intelligence services and other individuals (who may disguise their real identity) actively seek information from Defence personnel and their spouses, partners, family members and friends about Defence capabilities, which may potentially harm Defence personnel, information and interests.

a. Defence personnel must not provide information in response to requests for information about Defence through digital channels without appropriate clearance. Requests from media must be referred to Defence Media and requests from the public are to be referred to the Defence website. Suspicious contacts must be reported to the Defence Security and Vetting Service.

7.12 To meet individual security responsibilities, Defence personnel must abide by the eSafety Commissioner's eSafety Guide; Defence Security and Vetting Service's Social Media Security intranet page and top tips to help protect you on social media; the Australian Cyber Security Centre's Personal Cyber Security: First Steps Guide; Personal Cyber Security: Next Steps Guide; Personal Cyber Security: Advanced Steps Guide; security tips for personal devices and easy steps to secure your online information; the Australian Security Intelligence Organisation's Think Before You Link guidance; and the Australian Public Service Commission's guidance on the use of social media. In addition, Defence personnel must keep their unofficial social media accounts secure by:

a. applying the highest privacy and security settings available;

b. choosing separate and complex passwords for each account, changing them regularly (approximately every three months), using two-factor authentication where possible, logging out when not in use, and not allowing web browsers to store passwords;

c. turning off geotagging and location-based social networking to avoid sharing geographical details of where media such as photographs, video, websites and SMS messages were taken; and

d. not friending/connecting with people unknown to them.

7.13 Defence personnel are encouraged to talk to their spouses, partners and family members about the importance of maintaining secure social media accounts, including that they:

a. do not post operationally sensitive information (such as deployment dates, locations etc.) or tag Defence personnel in their posts;

b. apply the highest privacy and security settings available;

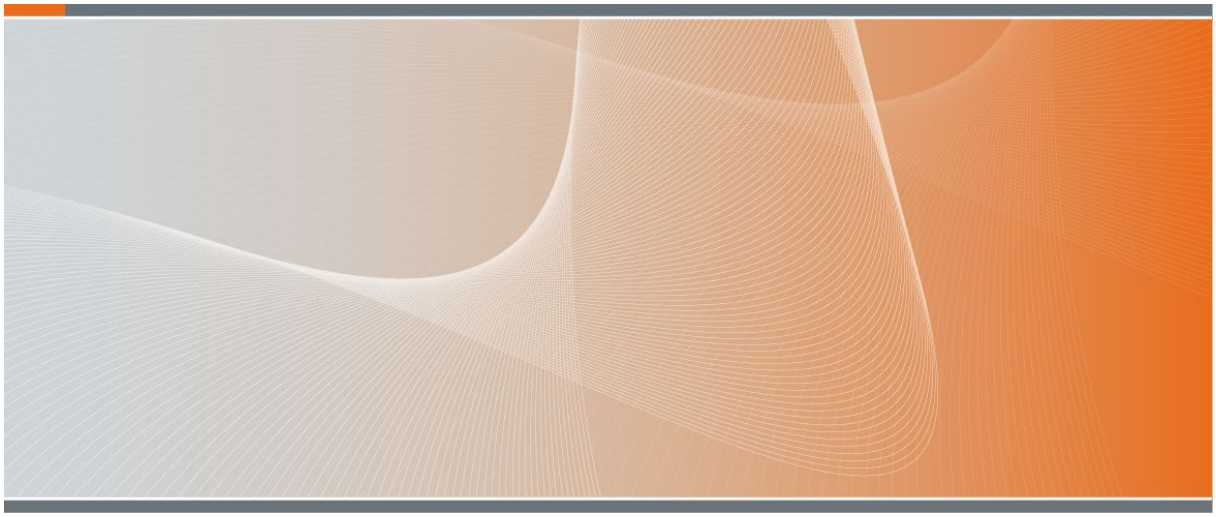
c. carefully consider the type and amount of information they post, including restricting personal information on their accounts (such as home or work address, phone numbers and place of employment etc.); and

d. choose separate and complex passwords for each account, change them regularly (approximately every three months), use two-factor authentication where possible, log out when not in use, and do not allow web browsers to store passwords.

7.14 For further information, refer to the Personal Social Media Guide on the Defence Social Media intranet page, or contact the Defence Social Media Hub.

Australian Government
Department of Defence

DEFENCE MEDIA AND COMMUNICATION POLICY



s22

10 August 2021

s22

SOCIAL MEDIA

1.30 Official Defence social media accounts must comply with Defence's strategic messaging and Defence Values and Behaviours.

s22

1.31 Ministerial and Executive Coordination and Communication (MECC) Division will set the overarching policy framework for, and provide the necessary support to manage and monitor official Defence social media accounts.

1.32 Groups and Services are responsible for managing their respective official social media accounts, as described in the Defence Media and Communication Guide and the Social Media Playbook.

s22

s22

SOCIAL MEDIA

1.63 Defence personnel using unofficial social media accounts will uphold their security and professional responsibilities as described in the Defence Media and Communication Guide and the Personal Social Media Guide; and comply with legislation, policy, guidance and Defence Values and Behaviours.