

APS People Policy

OUTSIDE WORK AND POLITICAL ACTIVITIES

Contents

Purpose 1
Application 1
Principles 1
Outside work during leave 3
Code of Conduct 4
Regular review 4
s22

Purpose

Defence Australian Public Service (APS) employees may only engage in outside work (paid or unpaid) after obtaining approval to do so from their supervisor. Employees who are considering outside work should discuss their plans with their supervisor before making any commitments to outside employers.

Application

1. This policy supersedes previous policies or guidance related to outside work and political activities.
2. This policy applies to all Defence APS employees and Australian Defence Force (ADF) supervisors of Defence APS employees.
3. APS employees and their managers must comply with this policy when making related decisions. More information is in the Version Control and Authority section of this policy.

Principles

4. In general, APS employees are able to:

a. engage in work in addition to Defence employment provided it remains within the principles for outside work, and

b. involve themselves in outside activities of a voluntary and unpaid nature unless there is a clear conflict with the requirements of the APS Code of Conduct.

5. Outside work is other employment (paid or unpaid) or volunteer activities undertaken by an APS employee in addition to their official duties or while on paid or unpaid leave from Defence.

a. Examples of outside work include running a business from home, directorship of a company, driving a taxi, working for a consultancy company, serving on the committee of a sporting association, volunteering as a fire fighter, or coordinating charity work being delivered by a community organisation.

b. An employee seeking election for a local council must also seek permission to engage in employment in addition to their Commonwealth employment.

6. Employees are required to discuss the proposed outside work with their supervisor before engaging in outside work.

7. Employees are expected to carefully examine their personal and normal employment circumstances before undertaking outside work to ensure there is no adverse impact on their work performance, the workplace, or operational requirements by participating in outside work.

8. Employees, supervisors and managers must assess conflicts of interest from both a Defence-wide perspective and a workplace perspective, considering whether a real or apparent conflict may exist.

9. If the supervisor has any doubt if a conflict of interest exists or not, or whether the risks associated with the conflict of interest can be adequately mitigated or not, they must, through the employee's supervisory line, consult the Principal Integrity Officer as per the Defence Instruction, Administration and Governance Provisions, AG5 – *Conflicts of interest and post separation employment*.

10. All Defence personnel must promptly declare any conflicts of interest (real or apparent) when they are identified using the AF220 Defence Conflict of Interest Declaration Form.

11. Employees, supervisors and managers need to regularly review any outside work performed to ensure that it continues to meet the policy principles and the requirements of the APS Code of Conduct.

12. If a manager concludes that the proposed outside work does not fit with the principles in this policy then the manager is authorised to direct that:

a. the employee does not engage in outside work, or

b. the employee may engage in outside work under certain conditions in respect of that employment, as determined by the manager.

13. Employees who have been directed not to engage in outside work, or whose outside work is the subject of other directions made by their manager, may seek a review of those directions.

14. The following are considered exceptions to outside work:

a. employment with a business, organisation or other Government agency, when undertaken as part of an official training and development scheme

b. training or duty as a member of the ADF Reserve

c. secondment to another Government agency.

15. When discussing proposed outside work (paid or unpaid) with employees, supervisors should consider the following:

a. Will or could the proposed work put the employee in a real or apparent conflict of interest with their official duties?

b. Could the proposed work adversely affect the efficiency of the employee in their Defence duties?

c. Will the proposed work be performed wholly within their private time?

d. Could the proposed work in any way adversely affect the operational requirements and/or the efficiency of the workplace?

e. Is there any risk that the proposed work could result in the improper use of Defence resources?

f. Could the proposed work lead to an improper use of Defence inside information?

g. Could the employee's duties in their normal employment with Defence, and/or the status, power or authority derived from it, be used to gain a benefit or advantage for the employee or any person in their proposed work?

16. A manager may need to consider the proposed outside work from a wider Defence perspective at a higher management level. In this case, the manager may consider:

a. a proper balance between the interest of Defence and the rights of the employee to lead a private life free of unnecessary restrictions

b. the impact on the workplace as a whole

c. the impact on others in the workplace, such as other employees who may be undertaking additional work, or other employees feeling that this employee is not contributing equally to the workplace.

17. The employee will usually be able to engage in the proposed outside work if the supervisor concludes that:

a. there is no real or apparent conflict of interest, or

b. following consultation with the Principal Integrity Officer, reasonable steps are agreed on to avoid, where possible, or manage any real or apparent conflicts of interest, including an agreement which restricts an employee from engaging in particular tasks that would conflict with their Defence APS employment.

Outside work during leave

18. Employees and decision-makers should give careful consideration to the reason leave exists as well as the normal consideration regarding engaging in other work when approving or recommending leave to undertake outside work.

19. Except in limited circumstances, outside employment, which includes Reserve service, is incompatible with being on Personal/Carer's leave. Personal/Carer's leave is provided specifically for employees to use when they are ill or injured or are required to care for and support an ill or injured family or household member

20. The circumstances when an employee may be able to perform Reserve service while on this form of leave are in the APS People Policy – Personal/Carer's Leave

21. Annual leave and Long Service Leave exist for the purpose of providing employees time away from their workplaces for rest and recreation. Engaging in outside work while on leave may defeat this purpose.

22. Supervisors and decision-makers need to be sensitive and balanced in reaching conclusions about what might or might not constitute an effective and useful break from Defence work, taking careful account of the interests and wishes of each employee.

23. Where an employee has been given a direction not to engage in outside work because of a concern that such work will be in conflict with Defence policy, leave for that purpose should not be approved.

24. Long service leave and leave without pay should generally not be approved for the purpose of 'trying out' a second career outside the public service. There are some circumstances where the approval of leave without pay to engage in outside work may be appropriate.

a. For example, Michael is an APS 5 employee in Sydney and his wife, a Navy Lieutenant, has been posted from HMAS Kuttabul to HMAS Coonawarra in Darwin. Michael wishes to accompany his wife on posting but has not been able to secure a job with Defence in Darwin. Michael therefore wishes to engage in employment other than with Defence while in Darwin. Michael's application for leave without pay may be approved for this purpose.

b. An employee may also take leave without pay to work for a non-Defence employer in the interests of Defence and of the APS as a whole.

Code of Conduct

25. As the potential for conflict of interest is of particular concern, employees, supervisors and managers should consider the provisions of the APS Code of Conduct when discussing and approving outside work. The key provisions of concern relate to:
    a. conflict of interest (real or apparent)
    b. improper use of Defence resources
    c. improper use of inside information
    d. improper use of Defence employment
    e. compliance with any lawful and reasonable direction by someone in Defence with the authority to give direction
    f. adherence to all applicable Australian laws.
26. In considering whether a conflict of interest may exist, or appear to exist, (particularly in relation to taking up company directorships) the employee, supervisor and manager will need to consider whether the organisation is:
    a. in, or in the process of entering into, a contractual relationship with the Commonwealth or its authorities
    b. in receipt of Commonwealth Government assistance, the entitlement to which depends on the exercise of discretion by a Commonwealth employee
    c. created to lobby Ministers, Members of Parliament, government departments and authorities
    d. in a regulatory relationship with Defence.
27. Unpaid voluntary work is less likely to result in a conflict of interest, although may still be possible. For example, voluntary work for political organisations, voluntary work for political lobby groups, or voluntary work for organisations not expressing their views in a lawful manner.
28. Employees, supervisors and managers should be aware that sanctions may be imposed on an employee who is found to have breached the APS Code of Conduct.
29. Managers and supervisors need to be careful not to breach the APS Code of Conduct themselves by ignoring the effects of an employee's outside work on the workplace, ignoring an employee's misuse of Defence time and/or resources to conduct outside activities, or failing to direct an employee not to engage in outside work when appropriate.
30. Employees failing to comply with a direction not to engage in outside work or to engage in the work under certain conditions imposed by a manager may be in breach of the APS Code of Conduct.

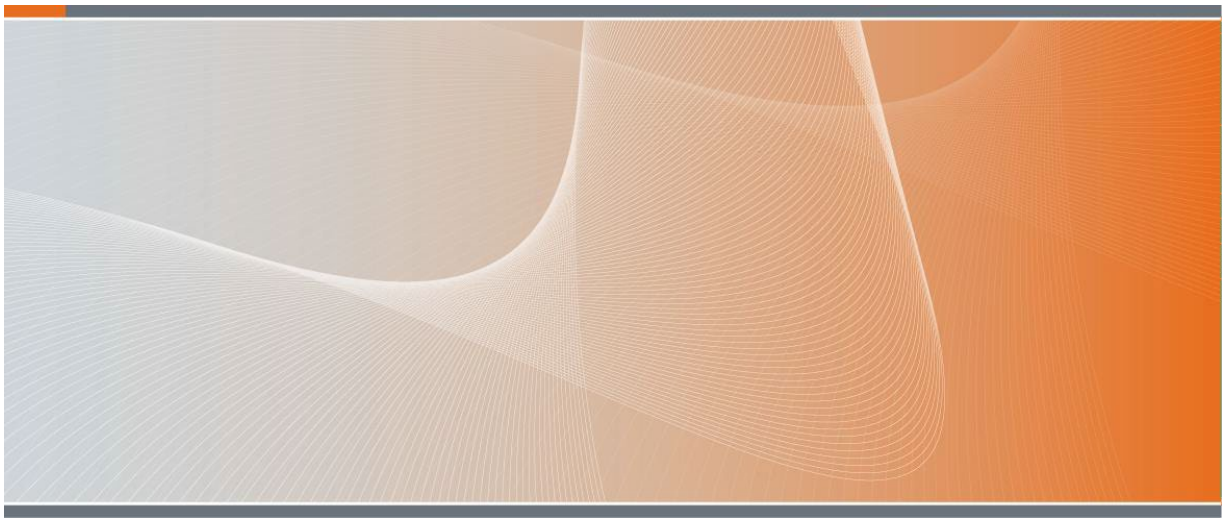
Regular review

31. Managers and supervisors are to monitor and review outside work arrangements:
    a. as part of the annual and mid-cycle performance exchange
    b. when negotiating a new performance agreement
    c. when an issue arises that may be associated with the impact of the outside work, such as unsatisfactory performance, the potential for a conflict of interest arises, or improper use of Defence resources
    d. when a new supervisor is appointed to the work team.

s22 [redacted]

Defence FOI 715/26/27
Document 2

DEFENCE MEDIA AND COMMUNICATION GUIDE



Cleared by Rowena Bain
First Assistant Secretary Ministerial and Executive Coordination and Communication

Department of Defence
CANBERRA ACT 2600

12 May 2022

Version 1.1 (issued 16 May 2022)

CHAPTER 3 – RELEASING OFFICIAL CONTENT OR MAKING PUBLIC COMMENT ON DEFENCE MATTERS

3.1 All content released by Defence, or Defence personnel, is considered official. Defence's external messaging must be consistent and delivered to the public in a coordinated, appropriate and timely way by trained and authorised Defence spokespeople.

3.2 Public comment by Defence personnel is the provision of official content to individuals or organisations external to Defence or for use in Defence publications. This includes, but is not limited to, social media, media releases, media responses, interviews, podcasts, background briefings, informal briefings, documents, letters to the editor, opinion pieces, articles, journals, academic/educational/research papers, professional military education parties, public briefings, speeches, lectures, presentations, seminars, workshops, conferences, commentary, imagery (including photographs and videos), audio, internet sites, mobile networks and self-contained works.

a. When official content is authored by Defence personnel, who have approval from their chain-of-command to identify themselves as a Defence employee, this information represents the views of the Government and Defence – not an individual's view – and must be apolitical in nature.

b. Defence personnel are not authorised to make public comment without approvals if doing so identifies them in any way as a Defence official – even if the views they express are their own.

c. All activities with actual or potential media or public interest (see paragraph 3.2 above) must be recorded in the Defence Activity and Engagement Tracker (the 'Tracker') in accordance with paragraphs 2.16-2.21 in Chapter 2 – Engagement with the Media.

3.3 Defence personnel releasing official content or making public comment on behalf of Defence must be authorised to do so and ensure content and comments are consistent with the position of the Government and Defence. Defence's communication efforts will take into account accessibility considerations for our diverse audiences.

3.4 Unless previously authorised, Defence personnel approached by the media for comment, must not engage in conversation specific to the matter and immediately refer the enquiry to Defence Media.

a. Defence involvement in public displays, events or recruitment activities is to be managed in accordance with paragraph 2.25 in Chapter 2 – Engagement with the Media.

b. Defence personnel must also register all unplanned and unauthorised media in the Defence Media Contact Register in accordance with the Defence Media and Communication Policy and paragraph 2.12 in Chapter 2 – Engagement with the Media.

3.5 Defence spokespeople must be a subject matter expert for the topic of the media engagement, who voluntarily agree to speak on behalf of Defence. Defence spokespeople are to be provided with appropriate media training in accordance with paragraphs 2.13-2.15 in Chapter 2 – Engagement with the Media.

s22



APPROVAL TO RELEASE OFFICIAL CONTENT OR MAKE PUBLIC COMMENT ON BEHALF OF DEFENCE

3.8 Defence personnel must only release information that is:

a. not protected by a security classification, or a protective, confidentiality or privacy marking;

b. not likely to compromise operational security, an individual's privacy without their prior consent, Australia's international relationships, the safety of Defence personnel or their families, or risk the waiving of legal professional privilege;

c. compliant with relevant legislation, policy and guidance;

d. consistent with the position of the Government and Defence;

e. apolitical in nature and will not be used for political purposes in any way contrary to Defence's apolitical standing;

f. about a major matter of policy, procurement or Service deployment which has been previously announced by the Government;

g. not speculation; and

h. authorised for release in accordance with the Defence Media and Communication Policy and this Guide.

3.9 Defence spokespeople must not provide comment on any matter that is outside the boundaries for which the interview was approved, and should take the question on notice or refer the matter to Defence Media, as appropriate.

3.10 Defence personnel are to only release official content or make public comment that has been authorised. Unless subject to an SES Band 1 or 1-Star officer-approved communication plan, military public affairs plan or public affairs guidance, engagement with the media or external parties for activities specified at paragraph

3.2, in either a private or official capacity, requires clearance from the responsible SES Band 2 or 2-Star officer (at a minimum) and forwarded to Defence Media for final Defence clearances in accordance with paragraphs 2.10-2.11 in chapter 2 – Engagement with the Media. The Director Defence Media has authority to lower the clearance level to an SES Band 1 or 1-Star officer (at a minimum) on a case-by-case basis.

3.11 Content developed for Service newspapers requires clearance by the relevant Service headquarters prior to publishing.

3.12 Where appropriate, Defence spokespeople identified by name in media releases must be pre-approved and prepared to conduct media interviews during the media release clearance phase.

UNAUTHORISED DISCLOSURE AND LEGISLATIVE COMPLIANCE

3.13 Unauthorised disclosure of information may constitute a security breach under the Defence Security Principles Framework (DSPF), and may also constitute a breach of the requirements of legislation. Relevant legislation for a release might include any of the *Defence Force Discipline Act 1982*; *Defence Inquiry Regulations 2018*; *Public Service Regulations 1999* (regulation 2.1); *Crimes Act 1914*; *Privacy Act 1988*; *Freedom of Information Act 1982*; *Espionage and Foreign Interference Act 2018*; and the Australian Public Service Code of Conduct.

a. Instances where classified, personal, commercial or sensitive information has been disclosed to the media or public will be investigated by the Defence Security and Vetting Service and may be referred to law enforcement agencies. Defence personnel who are found to have disclosed classified, personal or sensitive information to the media or public will be subject to administrative, disciplinary or criminal action as appropriate. This also applies to contractors in accordance with the scope of this Guide.

3.14 This Guide sets out the approvals that must be sought by Defence personnel before information is released outside Defence. If there are instructions mandating approvals to be sought prior to release and it appears that they have been disregarded by Defence personnel, the matter may also be referred for a fact find and relevant Code of Conduct, disciplinary or contract actions.

3.15 Former Defence personnel must comply with all relevant legislative requirements, including but not limited to those regarding:

a. the unauthorised disclosure of information; and

b. protection of intellectual property rights (copyright, trademarks, etc.).

3.16 Content for web publishing must comply with Web Content Accessibility Guidelines 2.2, Defence Web Estate Manual (WEBMAN) and the Digital Transformation Agency.

3.17 Content approved for public release must be archived in accordance with Records Management Policy Manual (RECMAN) and the *Archives Act 1983*.

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 information and communications technology resources, refer to the ICT Policy Framework.

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
Defence

DEFENCE INSTRUCTION

This Defence Instruction is issued by us pursuant to subsection 11(1) of the *Defence Act 1903* and is effective as at today's date. *Defence Instruction* dated 27 September 2024 is hereby revoked.



s22

Greg Moriarty, AO
Secretary
Department of Defence
28 January 2026

s22

David Johnston, AC
Admiral, RAN
Chief of the Defence Force
19 January 2026

To defend Australia and its national interests in order to advance Australia's security and prosperity
www.defence.gov.au

PURPOSE

1. This is a Defence Instruction for the purposes of section 11 of the *Defence Act 1903*. Its primary purpose is to support the Secretary of Defence (the Secretary) and the Chief of the Defence Force (CDF) to discharge their responsibilities under subsection 10(1) of the *Defence Act 1903*, to jointly administer the Australian Defence Force.

2. Its secondary purpose is to support the Secretary to discharge the Secretary's responsibility under paragraph 57(2) (a) of the *Public Service Act 1999* to manage the affairs of Defence in an efficient, effective, economical and ethical manner. To the extent necessary, it draws authority from subsection 20(1) of the *Public Service Act 1999*.

3. This Defence Instruction:

   a. includes prescribed and proscribed (mandatory) provisions specified by the use of the words '**must**' or '**must not**' that apply to all or specified Defence personnel.

   b. prevails over any Defence document that is not issued under section 11 of the *Defence Act 1903* or under section 20A of the *Public Governance Performance and Accountability Act 2013*, so far as it relates to matters of an administrative nature.

   c. is not intended to duplicate powers, functions and duties that already exist in legislation.

   d. does not provide for and is not intended to limit the implied discretionary power of Accountable Officers to issue, or authorise the issue of, procedures and guidelines.

INTERIM DEFENCE INSTRUCTION

4. **Interim Defence Instructions** may be used as a temporary measure (for up to 12 months). An Interim Defence Instruction can amend or revoke provisions of this Defence Instruction or make a new provision. They prevail over extant provisions of this Defence Instruction, to the extent of any inconsistency until the Interim Defence Instruction expires, or is revoked, and its contents incorporated into this Defence Instruction.

WHAT DOES THIS DEFENCE INSTRUCTION MEAN TO ME

5. **If you are a Defence member:**

   a. this Defence Instruction contains 'general orders' for the purposes of the *Defence Force Discipline Act 1982* (indicated by use of the words '**must**' or '**must not'**).

   b. failure to comply with a mandatory provision in this Defence Instruction that applies to a Defence member may result in administrative or disciplinary action.

6. **If you are a Defence Australian Public Service (APS) employee:**

a. this Defence Instruction contains lawful and reasonable directions (indicated by use of the words '**must**' or '**must not'**) for the purpose of subsection 13(5) of the *Public Service Act 1999.*

b. failure to comply with a mandatory provision of this Defence Instruction that applies to a Defence APS employee may result in an investigation and sanction as provided for in subsection 15(1) of the *Public Service Act 1999*. These may range from reprimand to termination of employment.

7. **If you are a person engaged under a contract, another Commonwealth Department secondee, or a foreign military exchange officer:** your contract or your secondment or exchange arrangement may require you to comply with:

a. the mandatory provisions of this Defence Instruction; and

b. any administrative policies and directions issued pursuant to this Defence Instruction where they are directly relevant to the work you will be performing for Defence.

KEY ROLES RELATING TO THIS DEFENCE INSTRUCTION

8. The **Secretary** and the **CDF** provide the highest level of authority to jointly issue Defence Instructions and *Interim Defence Instructions*.

9. By *delegation of power* the **Associate Secretary** and the **Vice Chief of the Defence Force** hold the next level delegation to jointly issue Defence Instructions (including *Interim Defence Instruction*). If, however, it is proposed that a Defence Instruction (including an Interim Defence Instruction) contain a grant, to an Accountable Officer, or other specified appointment, of a power to issue directions binding on Defence personnel across the Defence enterprise, the Defence Instruction will need to be issued by the Secretary and CDF. This is because only the Secretary and the CDF may delegate their power to issue Defence Instructions under subsection 120A(3A) of the *Defence Act 1903.*

10. **Accountable Officers** are, in accordance with Administration and Governance Provision 1 of this Defence Instruction (AG1), accountable to the Secretary and the CDF for:

a. ensuring their provisions in this Defence Instruction are fit for purpose; and

b. effectively promoting realisation of the Defence strategic outcomes for which they are responsible.

11. The **Associate Secretary** is accountable to the Secretary and the CDF for developing, issuing and maintaining arrangements for administrative policies (the *Administrative Policy Arrangements*).

12. On behalf of the Associate Secretary, and in accordance with the *Administrative Policy Arrangements*, the **First Assistant Secretary Governance, Planning and Performance Division (FAS GPP)** is responsible for coordinating the process of amending or revoking and re-issuing this Defence Instruction annually. By *delegation of power*, FAS GPP may revoke Defence Instructions (including Interim Defence Instructions).

13. **Chief Counsel** is responsible for providing legal advice and clearance of Defence

Instructions (including Interim Defence Instructions) prior to submission to the Secretary and the CDF (or their delegates) for approval to issue.

14. **Group Heads and Service Chiefs** are responsible for properly promoting and implementing this Defence Instruction and any administrative policies and directions (where applicable) within their Group or Service.

ADMINISTRATION AND GOVERNANCE PROVISIONS

Title:	AG5 – Conflicts of interest
Object:	AG5 mandates conduct relating to declaring, recording and managing conflicts of interest in Defence.
Accountable Officer:	Deputy Secretary Governance
Policy Owner:	Principal Integrity Officer (First Assistant Secretary Defence Integrity)
Policy Contact:	Director Integrity Policy
Cancellations:	NIL

AG5.1 All Defence personnel **must** act transparently when making work-related decisions, reflecting the probity and ethical standards of the Commonwealth and Defence, including adherence to Defence Values and Behaviours.

AG5.2 Defence personnel **must not**, either by act or omission:

a. make improper use of their authority, status, power or position in order to solicit or obtain a benefit or advantage (or cause a disadvantage) for themselves or any other person or group (including partners, relatives, friends, associates and any person that does or may do business with Defence);

b. use Defence resources (including official information not in the public domain) to gain, or seek to gain, a private benefit or advantage (or cause a disadvantage) for themselves or any other person or group;

c. accept any gift, benefit or sponsorship that might lead a reasonable person to view such acceptance as a conflict of interest;

d. behave in a manner which could be perceived as favouritism, bias, coercion or corruption; or

e. take improper advantage of their official position or access to privileged information gained in that position, when seeking or participating in employment, business or other activities outside of Defence.

AG5.3 All Defence personnel **must** regularly assess whether they have an actual or perceived conflict of interest, including, but not limited to when they change roles, have another role or competing duty, experience a change in personal circumstance, or undertake secondary employment or post-separation employment opportunities.

AG5.4 The Principal Integrity Officer (PIO) **must** be consulted where there is any doubt about whether:

a. a conflict of interest exists or not; or

b. the risks associated with the conflict of interest can be adequately mitigated or not.

AG5.5 All Defence personnel **must** take reasonable steps to avoid situations where their private financial interests, relationships (intimate or professional), and other interests (or those of *immediate family members*) could compete, or could be perceived to compete, with their official functions or duties.

AG5.6 All Defence personnel **must** promptly declare any conflicts of interest (actual or perceived) as and when they are identified, using the *AF220 Defence Conflict of Interest Declaration Form.*

ANNUAL DECLARATION OF INTEREST

AG5.7 An annual declaration of interests, using the *AF220 Defence Conflict of Interest Declaration Form*, **must** be made by 31 October by:

a. members of the Senior Leadership Group (SLG) including all Star Ranked Officers, Star Ranked SERCAT 5 Reserve Officers, Senior Executive Service Officers, Medical Officers Class 5 and 6, and Chiefs of Divisions;

b. anyone below SLG level who is designated by their Group Head or Service Chief because the position they occupy, their responsibilities or their level of decision-making require them to be particularly transparent about their financial and personal interests; and

c. all external committee members and chairs.

AG5.8 The PIO **must** be notified of the positons identified at AG5.7b.

AG5.9 A declaration of interest **must** also be made by:

a. Star Ranked SERCAT 3 Reserve Officers, within two weeks of the commencement of any specified task/official functions or duties and if applicable, annually thereafter in line with AG5.7;

b. newly promoted SLG or SLG who have transitioned to a new role, within two weeks of commencing and annually thereafter in line with AG5.7; and

c. anyone acting in one of the positions identified at AG5.7 for a period of three months or more, within two weeks of commencing their acting duties and annually thereafter in line with AG5.7.

PROCUREMENT

AG5.10 Defence personnel responsible for a procurement outcome with an expected value at or above $125,000 inclusive of the Goods And Services Tax, **must** ensure that Defence personnel involved in a procurement complete an AF220 Defence Conflict of Interest Declaration Form, regardless of whether a conflict of interest exists.

a. At a minimum, a declaration must be made by Defence personnel at the following stages: prior to the approval of an Endorsement to Proceed; prior to commencing an

evaluation of any response to an approach to market and prior to exercising the '*Commitment Approval – Public Governance Performance and Accountability Act 2013* section 23(3)' delegation.

b. Defence personnel are not required to complete more than one declaration for a procurement unless circumstances arise that change an existing declaration or create a new conflict of interest but must consider at each of the stages listed at AG5.10a if circumstances have changed that warrant a new declaration to be made.

CONTRACT MANAGEMENT

AG5.11 When performing the role of a Contract Manager, Contract Authority, Commonwealth Representative (or equivalent), Defence personnel **must** regularly assess whether they have a conflict of interest in performing their official functions or duties. Where a conflict of interest exists or arises, they **must** immediately declare it using the AF220 Defence Conflict of Interest Declaration Form.

RECRUITMENT

AG5.12 Defence personnel must complete an AF220 Defence Conflict of Interest Declaration Form:

a. when performing the role of Chairperson or Panel Member for an APS Merit-based Recruitment Activity, when the list of candidates is known but before accessing applications; and

b. when preparing and/or signing the Section 25 or 26 paperwork, before approving a transfer outside of an APS Merit-based Recruitment Activity.

GRANTS

AG5.13 Defence personnel must complete an AF220 Defence Conflict of Interest Declaration Form:

a. before participating in an assessment of grant applications; and

b. before making a decision to approve or not approve a grant application (including consideration of any variations).

POST-SEPARATION EMPLOYMENT

AG5.14 Defence personnel **must** declare any offer of post-separation employment with a prospective employer that provides goods or services to Defence, is a member of a standing offer panel or that otherwise may give rise to a conflict of interest (actual or perceived), using the AF220 Defence Conflict of Interest Declaration Form, as soon as practicable and before accepting the offer.

AG5.15 Defence personnel **must** (in writing), notify their prospective employer of their conflict of interest disclosure obligations to Defence on receipt of an offer of employment. Defence personnel **must** retain written evidence of the notification and provide a copy to the relevant business area.

AG5.16 Defence personnel must (in writing), notify their prospective employer of any management strategies or restrictions imposed by Defence, before accepting an

offer of post-separation employment. Defence personnel **must** retain written evidence of the notification and provide a copy to the relevant business area.

INTIMATE RELATIONSHIPS

AG5.17 All Defence personnel **must** consider whether their current or former intimate relationship/s may give rise to a conflict of interest (actual or perceived) and if so, **must** declare these in writing to their manager/commander. Both the declarant and the manager/commander **must** retain written evidence of the declaration.

GIFTS, BENEFITS AND SPONSORSHIP

AG5.18 All Defence personnel **must** comply with Defence's Gifts, Benefits and Sponsorship policies.

LOBBYING CODE OF CONDUCT

AG5.19 All Defence personnel **must** comply with the Australian Government Lobbying Code of Conduct.

MANAGING CONFLICTS OF INTERESTS

AG5.20 Defence personnel **must** promptly submit an AF220 Defence Conflict of Interest Declaration Form through to the appropriate Decision Maker for a decision on the management of any conflict of interest declared.

AG5.21 Written consent **must** be obtained from third parties by using the Declaration of Interest Third Party Release Form, if Defence personnel are proposing to disclose a third party's personal information in an AF220 Defence Conflict of Interest Declaration Form.

AG5.22 The Decision Maker must ensure that a copy of the completed AF220 Defence Conflict of Interest Declaration Form is provided to the relevant business area for central oversight and implementation of management strategies, and a copy of the form **must** be submitted to Defence Integrity Division and the declarant.

For the purpose of AG5:

A **conflict of interest** refers to any situation where there is, could be or may appear to be, a conflict between an individual's private interests (including those of their immediate family) and their public duties and responsibilities. Information to assist Defence personnel to apply this instruction can be found *here*.

An **actual (real) conflict of interest** exists where you have a personal interest or competing duty that could affect or be affected by the way you perform your official functions or duties.

A **perceived (apparent) conflict of interest** exists where a reasonable person might think that you have a personal interest, relationship or competing duty that could affect or be affected by the way you perform your official functions or duties, even though there is no actual conflict of interest.

A **'material' personal interest** has the potential to give rise to an actual or perceived conflict of interest. Personal interests do not give rise to a conflict of interest unless there is a real or sensible possibility of conflict (not simply a remote or theoretical possibility of conflict).

APS Merit-based Recruitment Activity means an APS recruitment process for ongoing positions or non-ongoing positions advertised for 12 months or more

where:

- All eligible members of the community had a reasonable opportunity to apply.
- Candidates were assessed using a competitive selection process.
- Assessment was based on how well candidates' work-related qualities matched the genuine requirements of the role.
- Focus was on each candidate's capacity to achieve outcomes.
- Merit was the primary consideration in the final decision.

Defence personnel means all Australian Public Service employees in the Department of Defence, Defence locally engaged employees, Defence civilians, all Australian Defence Force members and their equivalents from other Defence organisations on exchange to Defence, external committee members and person/s engaged under a contract including a contractor, consultant or outsourced service provider as defined in the *Glossary - Accountable Authority . Instructions and Delegations*.

Manager/Commander means Defence personnel who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager or commander may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Decision Maker refers the Defence official responsible for evaluating actual and perceived conflicts of interest and mandating appropriate management strategies to mitigate risk. Further guidance can be found *here*.