Australian Government
Department of Defence

DEFENCE INSTRUCTIONS (GENERAL)

Editorial correction

ADMIN 08–2 *Use of social media by Defence personnel*
AMDT NO 2

Department of Defence
CANBERRA ACT 2600

Issued with the authority of the Chief of the Defence Force and the Secretary of the Department of Defence pursuant to section 9A of the *Defence Act 1903* for members of the Australian Defence Force.

Issued with the authority of the Secretary pursuant to section 20 of the *Public Service Act 1999* for Department of Defence Australian Public Service employees.

Dennis Richardson
Secretary

D.J. HURLEY, AC, DSC
General
Chief of the Defence Force

Sponsor:

Deputy Secretary Defence Support and Reform

Sponsor contact:

Assistant Secretary Corporate Communications

Effective Date: 16 January 2013

Review Date: 15 January 2016

Cancellation

DI(G) ADMIN 08–2 of 16 JAN 2013 (AL1) is cancelled.

USE OF SOCIAL MEDIA BY DEFENCE PERSONNEL

INTRODUCTION

1. This policy provides guidance on the use of social media by Defence personnel for the purpose of public engagement and to regulate the use of social media by Defence personnel where such use poses a reputational risk to Defence.

Within the Defence context, social media is defined as:

> *Digital tools that enable communication and sharing across the internet and that allow for the creation of user-generated content.*

IMPLEMENTATION

2. This Instruction should be read in conjunction with Defence Instruction (General) (DI(G)) ADMIN 08–1—*Public comment and dissemination of official information by Defence personnel*, which is the overarching policy instruction.

SCOPE

3. Social media offers people and organisations new ways to communicate with the public, with each other and with stakeholders. Social media is merely a new communication channel and therefore the same principles for guiding Defence personnel in their use of more traditional public-facing engagement still apply.

4. Many Defence personnel mistakenly believe that their comments and interactions on social media are private and anonymous. However, there is no guarantee of privacy and the concept of an individual's private identity and their Defence identity in social media can become blurred. Any inappropriate public comment may damage the reputation of Defence, a Group or Service, and/or an individual. Consequently, there can be no distinction between statements made officially on behalf of Defence, and professionally as a Defence employee or member of the Australian Defence Force (ADF).

5. Defence personnel are reminded that certain behaviour within a social media environment may amount to prejudicial conduct under the provisions of the *Defence Force Discipline Act 1982* (DFDA) (s 60) and the Australian Public Service (APS) Values and Code of Conduct, under the *Public Service Act 1999* and Regulation 2.1 of the Public Service Regulations.

POLICY STATEMENT

6. In this context, it should be noted that section 60 of the DFDA provides that a Defence member is guilty of an offence if the member does an act, or omits to perform an act, that is likely to prejudice the discipline of, or bring discredit on, the Defence Force.

7. In relation to the Public Service legislation it should be noted that obligations of Defence employees under the APS Code of Conduct include the requirement in subsection 13 (11) of the *Public Service Act 1999* provides that an 'APS employee must at all times behave in a way that upholds the APS Values and APS Employment Principles and the integrity and good reputation of the employee's Agency and the APS'. Regulation 2.1 of the Public Service Regulations deals with the disclosure of certain information obtained or generated in connection with a Defence employee's employment. Attention is also drawn to Australian Public Service Commission Circular 2012/1—*Revisions to the Commission's guidance on making public comment and participating online* which may be accessed at http://www.apsc.gov.au/publications-and-media/current-circulars-and-advices/2012/circular-20121.

8. Supervisors within Defence should ensure that any bullying complaints are managed in accordance with DI(G) PERS 35–3—*Management and reporting of unacceptable behaviour*, which outlines Defence procedures relating to unacceptable behaviour in the workplace. Failure to do so may risk Defence, and the supervisor, being exposed to bullying claims under the *Fair Work Act 2009*. Other Commonwealth, State and Territory criminal, workplace and discrimination legislation could also be applicable to inappropriate behaviour in social media.

9. This policy covers all official communication using social media, as well as private activities in social media where an individual can be identified as being a Defence employee or member of the ADF.

10. All Defence personnel must comply with the mandatory requirements of this policy. A mandatory requirement of this policy is identified through the use of the word **must**.

11. The mandatory requirements of this Instruction constitute a general order to Defence members for the purposes of the DFDA. Non-compliance with any mandatory requirement may result in disciplinary action being taken in accordance with the DFDA.

12. The mandatory requirements of this Instruction are a direction to Defence employees by the Secretary for the purpose of s 13(5) of the *Public Service Act 1999* (s 13(5) forms part of the APS Code of Conduct). Accordingly, non-compliance by Defence employees with any mandatory requirement of this Instruction will be referred for investigation and possible sanction in accordance with the *Public Service Act 1999*.

13. Defence contract managers must ensure that the requirement for external service providers to comply with the mandatory requirements of this Instruction is included in the terms of their contract.

14. Failure by an external service provider to comply with the mandatory requirements of this Instruction may result in a breach of contract.

15. Defence policy on the use of social media by Defence personnel is framed around the right to freedom of expression under Article 19(2) of the International Covenant on Civil and Political Rights, Commonwealth, State and Territory laws, Defence Instructions and APS Commission guidance. A list of associated guidance is in Annex A.

16. Defence's social media policy covers:

a. Defence-related, user-generated, content that is shared over the internet via technologies that promote engagement, sharing and collaboration;

b. Defence's official social media presences;

c. internet-based and mobile applications owned and operated by Defence (iArmy, internet-based Service games, iTunes/Android applications, etc); and

d. all other activities conducted by Defence personnel on social media networks, where their connection to Defence is apparent or may be identified.

RESPONSIBILITIES, MONITORING AND EVALUATION

17. On behalf of Defence the risk owner for organisational communication is the Chief Operating Officer. The Secretary and Chief of the Defence Force (CDF) Advisory Committee will regularly review Defence's social media activities as part of its annual review of the Defence Communication Plan. Amendments to this policy, the access to and practice of social media in Defence and other related matters, will be determined by the Secretary and CDF after discussion at the Secretary and CDF Advisory Committee.

18. For Group and Service-level communication, aimed at management and Command responsibilities, the risk owner for social media activities is the relevant Group Head or Service Chief. Some social media networks are part of the ongoing engagement that Groups and Services have with their own staff and the broader community. Within the guidelines established by this policy, the governance, responsibility and control of those social media activities will remain with the relevant Group or Service and be exercised through their existing arrangements.

COMPLIANCE

19. In line with section 60 of the DFDA and the Public Service provisions referred to in paragraphs 5., 6. and 7. above, Defence personnel **must not** post material that is offensive towards any group or person based on any personal traits, attributes, beliefs or practices that exploit, objectify or are derogatory of gender, ethnicity or religion. Such behaviour involving social media may amount to conduct that could constitute an offence against provisions of the DFDA, the *Public Service Act 1999* or amount to a breach of the APS Code of Conduct.

20. In addition, Defence personnel **must not** use official information in online forums or transmit it by other electronic means without prior approval and authorisation. When engaged in online forums or when sending information privately, Defence personnel **must** exercise judgment to ensure that no information breaches security or adversely affects the safety and wellbeing of Defence personnel and their families, or damages Defence's reputation and international relationships.

OFFICIAL COMMUNICATION

21. Only those authorised to comment may do so as an authorised spokesperson of Defence. The authorisation process for making public comment and the dissemination of official information using social media is pursuant to DI(G) ADMIN 08–1. The First Assistant Secretary Ministerial and Executive Coordination and Communication is the authorisation officer for 'Whole-of-Defence' social media presence and activities. The authorisation officer for social media presence at the Group and Service level is the relevant Service Chief or Group Head.

22. When an authorised Defence spokesperson engages in social media on behalf of the organisation they **must**:

a. disclose that they are an employee/contractor of Defence and use only their own identity or an approved official account or identity;

b. disclose and comment only on information in the public domain;

c. ensure that all content published is accurate, not misleading and that it complies with all relevant Defence policies;

d. ensure that they are not the first person to make an announcement (unless specifically authorised to do so);

e. comment only on their area of expertise and authority;

f. ensure that comments are respectful of the community in which they are interacting online;

g. adhere to the terms of use of the social media platform or site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines; and

h. ensure that appropriate consideration is given to the protection of the privacy of individuals named or depicted in Defence imagery.

23. Some social media sites allow visitors to make changes, contributions, or corrections to the information they host, such as Wikis. In circumstances where Defence cannot control the integrity of such information, particularly for Wikis in the public domain, Defence personnel **must not** post information relating to Defence or its activities. Such public Wikis **must not** be used as part of official Defence communication.

24. When Defence personnel engage in commentary on social media within their professional expertise and are identified or identifiable as Defence personnel, this is a form of official communication. In these cases, subparagraphs 22.a. to h. of this Instruction apply to their engagement with social media. Additionally, Defence personnel **must** provide a suitable disclaimer, such as 'The views expressed are mine alone and do not reflect the views of the Department of Defence.'

Record keeping for social media activities

25. Defence personnel must record all dealings with social media in accordance with *Defence Records Management Policy Manual* (POLMAN 3).

26. When deciding whether to capture social media material, Defence personnel **must** consider whether:

a. the social media provides evidence of Defence's business activities;

b. the records created in social media need to be captured into an appropriate records management system;

c. the records are already captured, for example, was a final version developed, approved, captured in the records management system and later posted to the social media site, or does the record exist only on the social media site; and

d. the content (especially where there are non-Commonwealth contributors) should it be captured and by whom.

27. For further advice and assistance on staff responsibilities to capture records, refer to the *Defence Records Management Policy Manual* (POLMAN 3), or contact the Freedom of Information and Information Management Branch.

Annexes:
A. Definitions
B. Relevant Legislation, Regulation, Instruction and policy for social media in Defence
C. Guidelines for engagement in social media by Defence personnel

DEFINITIONS

Authorised spokespeople. In line with advice provided in Defence Instruction (General) (DI(G)) ADMIN 08–1—*Public comment and dissemination of official information by Defence personnel*, where a Defence spokesperson is required for a media interview, this person will generally be selected by the Secretary, Chief of the Defence Force, Group Heads or Service Chiefs or their delegates and authorised by the Assistant Secretary Communication and Media. Wherever practicable, the selected spokesperson will also be the Defence subject matter expert for the specific issue in question.

Public Affairs Officers and Strategic Communication Advisers are authorised to liaise with the media and provide agreed background as required, provided they have cleared the information and imagery through the relevant Service, Group or regional commander or manager, or their deployed commander, and after authorisation for release from the Assistant Secretary Communication and Media or their delegate.

Defence personnel are authorised to provide factual official information to the media on routine Service and Group activities specific to their duties, following approval from their commanding officer, manager, or Group Head or Service Chief as appropriate and authorisation by Assistant Secretary Communication and Media or their delegate.

Defence employee means a person employed in the Department of Defence under section 22 of the *Public Service Act 1999*.

Defence member as defined in section 3 of the *Defence Force Discipline Act 1982* (DFDA) means:

a. a member of the Permanent Navy, the Regular Army of the Permanent Air Force; or

b. a member of the Reserves who:

(1) is rendering continuous full-time service; or

(2) is on duty or in uniform.

Defence personnel, for the purposes of this Instruction, includes all Australian Defence Force members and all Defence employees employed in the Department of Defence under the *Public Service Act 1999*. It also includes Defence locally engaged employees overseas, Defence civilians and the equivalents from other Defence organisations on exchange to Defence, as described in the definition of Defence personnel in the *The System of Defence Instructions Manual* (SoDIMAN), Chapter 1.

External service providers means contractors, consultants and professional service providers employed by Defence. External service providers who request permission to make public comment from Defence personnel on social media must be advised to seek independent legal advice before commenting, so that they do not unintentionally create a conflict of interest. Any conflict may be contrary to the terms of the contract under which they perform services for the Commonwealth.

Official communication occurs within official Defence social media channels which are channels established and run by Defence such as the Australian Army Facebook page. Any use of them by Defence personnel constitutes official communication.

Official information is defined in the Defence context as any fact, document or image in electronic or other form, which comes to the knowledge of, or into the possession of Defence personnel, in the course of their duties and:

- which carry a security, privacy or handling caveat;
- which are likely to be sensitive to policy, strategic or operational security issues; or
- the disclosure of which may reasonably be foreseen to be prejudicial to:
  - the effective working of Government, including the formulation or implementation of policies or programs;
  - the security or the defence of Australia and its interests; or
  - Defence's reputation.

This definition in no way limits the provisions of relevant regulations, including the *Crimes Act 1914*, the DFDA, the *Public Service Act 1999* and the Public Service Regulations 1999.

Public comment is the provision of information or images to individuals or organisations external to Defence.

Social Media is defined within the Defence context as: *Digital tools that enable communication and sharing across the internet and that allow for the creation of user-generated content*.

Wiki is a web page or set of pages that can be edited collaboratively, for example an online website which is created and edited by a large number of contributors across a variety of locations. Once people have appropriate permissions set by the Wiki owner, they can create pages and/or add to and alter existing pages.

RELEVANT LEGISLATION, REGULATION, INSTRUCTION AND POLICY FOR SOCIAL MEDIA IN DEFENCE

Defence social media policy should be read in conjunction with Defence Instruction (General) (DI(G)) ADMIN 08–1—*Public comment and dissemination of official information by Defence personnel*. Defence personnel should familiarise themselves with their terms of employment and all other applicable Defence policies and instructions, including (but not limited to):

1. Legislation:

   a. *Archives Act, 1983*.

   b. *Crimes Act 1914*.

   c. *Defence Act 1903.*

   d. *Defence Force Discipline Act 1982*, section 58.

   e. *Public Service Act 1999*, section 6.

   f. *Public Service Act 1999*, section 13.

2. Policy Guidance Documents and Regulation:

   a. Australian Public Service Values and Code of Conduct in practice, Australian Public Service Commission.

   b. Australian Public Service Commission Circular 2012/01—*Revisions to the Commission's guidance on making public comment and participating online*.

   c. *Defence Security Manual*, Part 1—Protective security and Part 2—Internet content.

3. Policy:

   a. DI(G) ADMIN 08–1—*Public comment and dissemination of official information by Defence personnel*.

   b. DI(G) CIS 6–1–001—*Appropriate and inappropriate use of Information and Communications Technology Resources*.

   c. DI(G) PERS 35–3—*Management and reporting of unacceptable behaviour*.

   d. *Defence Records Management Policy Manual* (POLMAN 3), Chapter 3—'Create, capture and describe'.

4. Guidelines:

   a. Operational Security and force preservation awareness training.

   b. Living the Service values.

   c. Defence Information Management Policy Instruction 2/2003—*Hand-held imagery metadata standard and procedures*.

GUIDELINES FOR ENGAGEMENT IN SOCIAL MEDIA BY DEFENCE PERSONNEL

1. As a matter of good practice Defence personnel who engage in social media **should**:

   a. consider carefully whether they should identify as a Defence member, a Defence employee or an external service provider contracted to Defence. Once identified, they will be perceived as representing the organisation in their online activities;

   b. consider disabling any automatic geo-tagging settings in their personal phones, cameras or mobile internet devices such as tablets and laptops;

   c. not join, or remain a member of, a group, forum, site or discussion that is involved in or promotes behaviour that is exploitative, objectifying or derogatory. Review the Department of Broadband, Communications and the Digital Economy website for information on Cybersafety;

   d. ensure the terms and conditions of use do not conflict with the Australian Public Service, departmental or Service policies. Content posted online potentially becomes public information and the property of the networking host;

   e. understand how to use privacy settings and preferences to restrict access to content;

   f. be aware that people online may disguise their real identity. Protect yourself, your family and your colleagues from the risk of identity fraud and other threats;

   g. be aware that social media websites are a common way for malicious adversaries to gather information about Defence projects, personnel and information. Adopting sound security practices, decreases the threat of malicious social engineering campaigns through this medium; and

   h. consider the use of the Australian Government's Cybersafety Help Button (available from www.dbcde.gov.au/) on their personal computers. The Cybersafety Help Button provides internet users with easy online access to Cybersafety information and assistance. The help button is a free application that is easily downloaded onto personal computers, mobile devices, and school and library networks.

2. Defence personnel **should** consider carefully whether to:

   a. disclose any personal information (where this cannot be protected), such as age, address, banking and financial information, passport, driver's licence and employment details, or information about work related activities and events;

   b. tag photos of colleagues or friends online without the permission of those in them;

   c. post images of members in uniform on non-Defence sites and, if so, consider the obligations associated with the applicable Service Dress manual; and

   d. post information or images that may damage your personal or professional reputation or that of your colleagues or family members now or in the future.

3. Defence personnel **should** be aware that a number of communities and individual websites exist whose purpose is to patrol social media activities seeking out sites, pages and comments that are contrary to Australian societal norms. These sites will often 'name and shame' individuals and organisations with racist, homophobic or intolerant views. On a number of occasions Defence's reputation has been damaged by the views of individual members or groups of members whose affiliation with Defence is known or identified.

Contacts

4. Should you have any questions associated with Social Media in Defence, or this social media policy, the Assistant Secretary Corporate Communication Branch is the appropriate point of contact for your query.