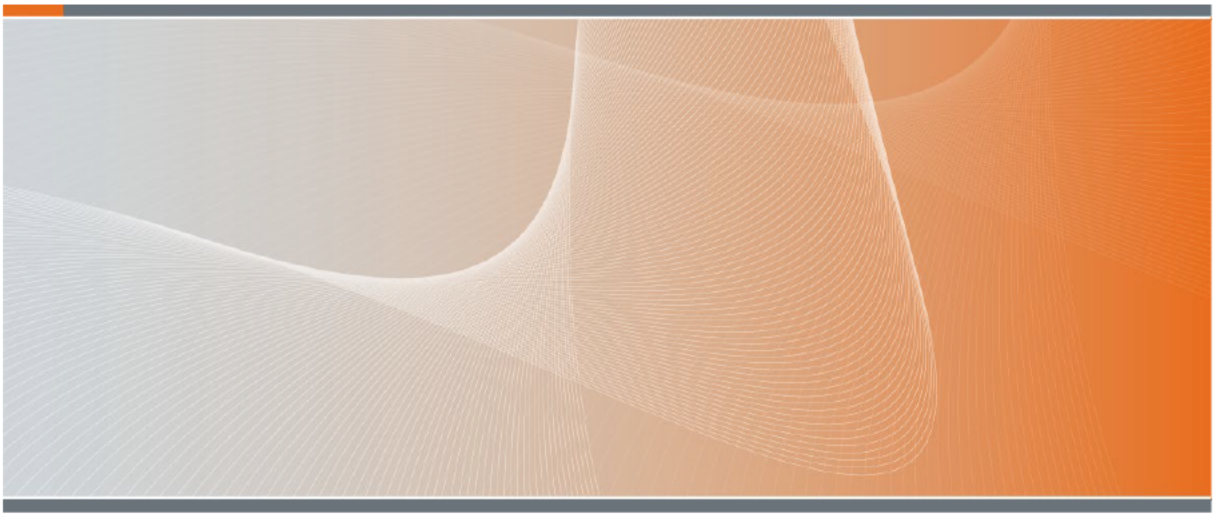
Australian Government
Department of Defence

DEFENCE MEDIA AND COMMUNICATION POLICY



s22 [redacted]

Steven Groves
Acting Associate Secretary

Department of Defence
CANBERRA ACT 2600

10 August 2021

DEFENCE MEDIA AND COMMUNICATION POLICY

Issued by: This Defence Media and Communication Policy (the ‘Policy’) has been issued by the Associate Secretary.

Purpose: This Policy describes Defence’s agreed approach for engaging with the media and governs all media and communication activities. This Policy is supported by a range of products on the Ministerial and Executive Coordination and Communication Division intranet page, including the Defence Communication Strategy and the Defence Media and Communication Guide, which must be read and adhered to, in conjunction with this Policy to enable Defence personnel to meet the expected outcomes.

Scope and applicability: This Policy is an administrative policy framework document. It applies to all Defence personnel.

The terms of a relevant contract may extend the application of this Policy to a person/s engaged under a contract.

Defence Instruction – Administrative policy should be read in conjunction with this Policy. In accordance with Defence Instruction – Administrative Policy, the Secretary and the CDF expect Defence personnel to comply with this Policy.

Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include the requirement to comply. If so, include such terms in the contract.

Management: This Policy will be reviewed within five years from its date of issue. A review may occur sooner to ensure it continues to meet the intended policy outcome/s.

Availability: This Policy is available at the Defence policy documents website. Its currency cannot be guaranteed if sourced from other locations. It is not available for public release.

Policy domain: Administration and Governance.

Accountable officer: Associate Secretary.

Policy owner: First Assistant Secretary Ministerial and Executive Coordination and Communication.

Policy contact: Assistant Secretary Media and Communication.

Cancellation: The publication of this Policy cancels any earlier editions of the Media and Communication Policy.

Definitions: Definitions that apply to this Policy are at Annex A.

DEFENCE MEDIA AND COMMUNICATION POLICY

POLICY STATEMENT

1.1 Defence aims to build public confidence and support for its mission, priorities, policies, activities and operational outcomes through the provision of effective communication and media engagement. This Defence Media and Communication Policy (this 'Policy') enhances Defence's reputation by enabling proactive, high quality, and well-coordinated media and communication products and activities in support of our ministers, the Government and the department.

1.2 Defence's media and communication function operates on a centralised control, decentralised execution model to deliver against the Defence Communication Strategy in accordance with this Policy.

1.3 This Policy acknowledges the unique and distinct Service brands, and the fundamental link to recruitment and warfighting efforts. This Policy supports Defence to manage its reputation through effective media and public engagement, with appropriate consideration of the associated risks.

POLICY RATIONALE

1.4 Public awareness and understanding of Defence policies and activities:

a. builds public confidence and support for Defence's mission, priorities, policies, activities and operational outcomes; and

b. strengthens Defence's credibility and reputation.

1.5 Unauthorised disclosure of information and online behaviour of Defence personnel can:

a. pose a risk to national security;

b. harm Defence personnel, information and national interests;

c. negatively impact Defence's reputation, Australia's international relationships, and the level of confidence the Australian community, the Government and industry has in Defence; and

d. put Defence personnel and their friends and family at risk of targeting from criminal and terrorist organisations, ideologically motivated groups, foreign intelligence services and other individuals seeking information about Defence capabilities.

1.6 Unauthorised endorsement of, and association with, external parties, real or perceived, may compromise Defence's impartiality, integrity and credibility.

1.7 The participation of the Prime Minister or a Defence portfolio minister in Defence events or activities provides the opportunity to reinforce strategic messaging.

1.8 Provision of accurate and authorised information to journalists and media organisations in a timely manner may help to prevent public perceptions of Defence being disproportionately shaped by speculation, misinformation or unbalanced reporting.

1.9 Achievement of media and communication outcomes will enhance confidence in Defence's ability to support its strategic priorities.

1.10 Effective, timely and authorised communication during a crisis or issue:

a. protects life, public safety and property;

b. preserves the integrity of the Department of Defence and the Australian Defence Force (ADF); and

c. enables the continued operation of Defence's core business.

1.11 Consistent application of Defence's brands helps:

a. tell our story;

b. uphold our reputation;

c. enhance awareness of the work we do; and

d. influence how Defence is perceived and valued by its people, stakeholders and the community.

EXPECTED OUTCOMES

1.12 Defence personnel comply with this Policy and requirements of the Defence Media and Communication Guide.

1.13 Defence personnel respond to requests for media and communication products and activities within assigned deadlines.

1.14 Where appropriate, media are provided opportunities to engage in what we do, including interacting with Defence senior leadership and being embedded in regional exercises and deployments.

1.15 Information provided by Defence is accurate, represents a whole-of-Defence view, and is aligned with Defence Values and Behaviours, policies and strategic communication objectives and plans.

1.16 Defence personnel actively incorporate the One Defence ethos by engaging early and effectively with relevant areas across the department to provide a single, well-coordinated and consistent enterprise response.

1.17 Effective, high-quality and well-coordinated media and communication products and activities in support of our ministers, the Government and the department that:

a. articulates the Government's defence policy and strategy; and

b. builds public confidence, understanding and support for its mission, priorities, policies and activities and operational outcomes.

1.18 Defence's credibility and reputation is strengthened through proactive and open communication and engagement with the media and the public.

1.19 Media and public engagement is authorised, apolitical and complies with legislation, policy and guidance. Defence protects classified and private information, operational security, international relationships and the safety of Defence personnel and their families. Defence personnel do not criticise or question the role or policy of the Government and the department to the media (including social media) or any other organisations.

1.20 Ministers and senior leaders are provided opportunities and support to communicate the work of Defence.

1.21 Defence's communication activities are evaluated to learn lessons and inform future communication efforts.

1.22 Defence brands are applied consistently; encapsulate who we are as an organisation; encompass our ethos and Defence Values and Behaviours; and embody our traditions and history.

1.23 Defence maintains impartiality and protects its credibility by not providing any express or explicit endorsements of any external party, its products, services or personnel, except when authorised in very exceptional circumstances.

1.24 Defence personnel understand their communication responsibilities and accountabilities.

DEFENCE MEDIA AND COMMUNICATION POLICY PRINCIPLES

1.25 The principles described in this Policy inform Defence personnel when engaging with the media and drafting media and communication products. The application of these principles, in conjunction with adherence to the requirements of the Defence Media and Communication Guide, will ensure Defence meets the expected outcomes of this Policy.

PRINCIPLE 1 – RELEASING OFFICIAL CONTENT OR MAKING PUBLIC COMMENT ON BEHALF OF DEFENCE MUST BE AUTHORISED

1.26 Defence personnel must only release official content or make public comment on behalf of Defence that is:

a. authorised for release in accordance with clearance authorities set out in the Defence Media and Communication Guide;

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

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

d. compliant with relevant legislation, policy and guidance[1];

e. consistent with the position of the Government and the department;

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

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

h. not speculation; and

i. in accordance with the Defence Media and Communication Guide.

MANAGEMENT OF MEDIA ENQUIRIES

1.27 Unless previously authorised, Defence personnel approached by the media for comment, must not comment on the matter and immediately refer the enquiry to Defence Media. Requests from the public are to be referred to the Defence website and suspicious contacts are to be reported to the Defence Security and Vetting Service.

DEFENCE MEDIA CONTACT REGISTER

1.28 Centralised visibility of contacts between journalists and media organisations with Defence officials supports a coordinated enterprise approach to Defence's strategic messaging as well as Defence's information security practices.

1.29 All Defence personnel must record Defence-related media interactions in the Defence Media Contact Register unless an authorised exemption applies, as described in the Defence Media and Communication Guide.

SOCIAL MEDIA

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

[1] Some legislative schemes provide for release of information separately to this Policy and the Defence Media and Communication Guide. Where those schemes are used, consideration should be given to whether the Defence Media and Communication Guide might also be followed, to deal with any public comment that follows the release of information.

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.

DIGITAL MEDIA

1.33 Defence digital media (including imagery and audio) intended for public release must be cleared through approved and appropriate internal channels before release, as described in the Defence Media and Communication Guide.

1.34 MECC is the central coordinating authority within Defence that receives public affairs imagery and associated products and coordinates final clearances for public release.

1.35 Outlined in section 82 of the *Defence Act 1903*, anyone making a sketch, drawing, photograph, picture or painting of any Defence installation in Australia must obtain prior approval from the authorised decision maker in Defence, as described in the Defence Media and Communication Guide.

1.36 Imagery for public release must remain an accurate representation of the subject matter. Minor adjustments of digital imagery such as cropping and tone/colour are permitted provided the integrity of the original image and context is maintained.

1.37 In circumstances where the original or alternative images are not suitable for public release, minor alternations to images are permitted only where it is necessary to manage operational and national security risks, protect the privacy of individuals or prevent viewer distress. Imagery is not to be altered for any other reason unless authorised in accordance with the Defence Media and Communication Guide.

1.38 Where an image is altered, the reason for the alteration and the name of the official authorising the alteration is to be clearly recorded in the associated metadata in accordance with Defence's handheld imagery metadata standard. The original unaltered image is to be appropriately classified and retained as part of Defence's official records.

ENTERTAINMENT AND NON-NEWS PROJECTS

1.39 Entertainment and non-news projects provide an opportunity for Defence to promote its strategic messaging beyond news media channels.

1.40 MECC will consider all requests for Defence support to entertainment and non-news projects on a discretionary basis against a range of criteria, as described in the Defence Media and Communication Guide.

a. The lead Group or Service is responsible for managing approved entertainment and non-news projects, as described in the Defence Media and Communication Guide.

DEFENCE ENDORSEMENT OF EXTERNAL PARTIES

1.41 To maintain Defence's impartiality and protect its credibility, Defence will generally not make any statement or provide any support that amounts to an endorsement or may be perceived as an endorsement of an external party, its products, services or personnel. The purchase of a product or service by Defence does not imply that Defence endorses that product, service or the supplier, nor should any other arrangement with a commercial entity suggest that Defence endorses that entity.

1.42 In exceptional circumstances, the responsible Group or Service may authorise a proposal for Defence endorsement where it is limited to factual statements and avoids commentary on performance or quality and it complies with the assessment criteria and clearance authority set out in the Defence Media and Communication Guide.

1.43 Endorsements provided by Defence must be limited to factual information regarding how Defence uses a product in the context of the Defence environment. All published statements must be time-stamped and be issued for limited use and for a specified period of time.

1.44 The purchase of a product or service by Defence does not imply that Defence endorses that product, service or the supplier, nor should any other arrangement with a commercial entity suggest that Defence endorses that entity.

1.45 Defence personnel involved in authorised endorsement or advocacy activities subject to overarching Commonwealth legislation or policy will undertake their duties with fairness and integrity and, as far as practicable, consistently apply endorsement principles as described in the Defence Media and Communication Guide.

GOVERNMENT ADVERTISING AND INFORMATION CAMPAIGNS

1.46 Defence's government advertising and information campaigns will comply with the Australian Government Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities and the Defence Media and Communication Guide.

ACCESSIBILITY

1.47 Defence's communication efforts will take into account accessibility considerations for our diverse audiences.

UNAUTHORISED DISCLOSURE

1.48 Unauthorised disclosures of classified, personal or sensitive information to the media or public can:

a. pose a risk to national security;

b. harm Defence personnel, information and Australia's national interests;

c. negatively impact Defence's reputation and the level of confidence the Australian community, the Government and industry has in Defence;

d. put Australia's international relationships and information sharing arrangements at risk; and

e. put Defence personnel and their friends and family at risk of targeting from criminal and terrorist organisations, ideologically motivated groups, foreign intelligence services and other individuals seeking information about Defence capabilities.

1.49 Unauthorised disclosures will be reported to the Defence Security and Vetting Service for investigation and where appropriate, disciplinary action will be taken. Matters will be referred to the Australian Federal Police where an incident involves actual or suspected criminal activity, such as the unauthorised disclosure of classified information.

PRINCIPLE 2 – COMMUNICATION IS RESPONSIVE

1.50 Defence personnel must respond to requests regarding media and communication products and activities as a high priority and within directed deadlines.

PRINCIPLE 3 – MEDIA OPPORTUNITIES WILL BE PROVIDED

1.51 Where appropriate, Defence will proactively seek and provide opportunities for media to engage in what we do, including interacting with Defence senior leadership and being embedded in operations, exercises and activities.

PRINCIPLE 4 – COMMUNICATION IS COORDINATED

1.52 Defence personnel actively incorporate the One Defence ethos by engaging early and effectively with all relevant areas across the department to provide a single, coordinated and consistent enterprise response.

1.53 MECC is the coordinating authority for apolitical media and communication for Defence portfolio ministers and the Defence enterprise.

PRINCIPLE 5 – DEFENCE SPOKESPEOPLE ARE TRAINED

1.54 MECC and military public affairs officers will provide appropriate media training and public affairs support for authorised Defence spokespeople, as described in the Defence Media and Communication Guide.

PRINCIPLE 6 – EVENTS AND ACTIVITIES ARE REGISTERED, PLANNED AND EVALUATED

1.55 All Defence operations, exercises, events and activities that have actual or potential media or public interest must be recorded in the Defence Activity and Engagement Tracker (the 'Tracker') by the lead Group or Service within assigned deadlines as described in the Defence Media and Communication Guide.

1.56 The lead Group or Service is to ensure that high-profile, large-scale, priority or significant Defence operations, exercises, events and activities that have actual or potential media or public interest are to have an appropriately cleared communication plan, military public affairs plan or public affairs guidance, where appropriate, that aligns with the Defence Communication Strategy and is prepared within assigned deadlines, as described in the Defence Media and Communication Guide.

1.57 Consistent with the Defence Communication Strategy, high-profile, large-scale, priority or significant communication activities will be evaluated against the achievement of communication objectives in the communication plan, military public affairs plans or public affairs guidance.

1.58 Evaluation of activities will be conducted by the lead Group or Service and finalised within assigned deadlines, as described in the Defence Media and Communication Guide.

PRINCIPLE 7 – MEDIA AND COMMUNICATION SUPPORT FOR THE PRIME MINISTER AND DEFENCE PORTFOLIO MINISTERS IS PRIORITISED

1.59 All Defence personnel will prioritise media and communication planning and support for all Defence events attended by the Prime Minister, a Defence portfolio minister, or another Government minister representing, ensuring they are at the centre of planning and support for these events, as described in the Defence Media and Communication Guide.

PRINCIPLE 8 – DEFENCE BRANDING IS CONSISTENT

1.60 Defence will apply its authorised brands, emblems, badges, symbols and iconography consistently and in compliance with relevant legislation, policy, branding principles and guidelines.

1.61 The Associate Secretary is the authority for the Department of Defence brand, which is to be used in accordance with the Guidelines on the use of the Commonwealth Coat of Arms, issued by the Department of the Prime Minister and Cabinet.

1.62 The Vice Chief of the Defence Force (VCDF) is the authority for the Australian Defence Force (ADF) brand and the respective Service Chiefs are the authority for the Navy, Army and Air Force brands.

PRINCIPLE 9 – DEFENCE PERSONNEL PARTICIPATING IN UNOFFICIAL MEDIA ACTIVITIES WILL COMPLY WITH SECURITY AND PROFESSIONAL RESPONSIBILITIES

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.

ENTERTAINMENT AND NON-NEWS PROJECTS

1.64 Defence personnel who are considering participating in entertainment and non-news projects in a private capacity (not on behalf of Defence) must obtain appropriate approval prior to submitting an application to an external party, conducting an audition or appearing in an entertainment and non-news project irrespective of whether their participation is undertaken while off-duty or on leave, as described in the Defence Media and Communication Guide.

KEY ROLES, FUNCTIONS AND RESPONSIBILITIES

1.65 **MECC Division**, within the Associate Secretary Group, is the coordinating authority for apolitical media and communication for Defence portfolio ministers and the Defence enterprise. MECC provides media, communication and public affairs expertise and services across the department to support Defence leaders, managers, commanders and personnel to promote Defence and protect and enhance its reputation.

1.66 **Military Public Affairs (MPA)** capabilities support MECC to deliver against the Defence Communication Strategy. The primary role of MPA elements within Defence is to support Defence operations, exercises and single-Service public affairs outcomes.

1.67 Where media and communication assistance is requested by MECC to support ministerial requirements, Service Chiefs are to prioritise and task their MPA capabilities accordingly.

1.68 **Commanders and Managers** are responsible for media and communication activities as described in the Defence Media and Communication Guide, including:

a. providing accurate and appropriately cleared information when required and authorised;

b. facilitating access by journalists and media organisations to Defence personnel and activities when required and authorised;

c. prioritising media and communication planning and support for all Defence events attended by the Prime Minister, a Defence portfolio minister, or another Government minister representing;

d. delivering media and communication activities and responses within required timeframes;

e. providing welfare support to individuals subjected to negative media commentary or coverage; and

f. providing welfare support to individuals subjected to negative media commentary or coverage.

1.69 Group Heads and Service Chiefs are responsible for:

a. managing the reputation of their respective Group or Service;

b. managing and coordinating their respective media events;

c. managing crisis and issues relevant to their Group or Service; and

d. managing all elements of approved entertainment or non-news projects.

Annex:

A Definitions

ANNEX A

DEFINITIONS

The following terms are defined in Defence Instruction – Administrative policy:

Accountable officer
Administrative policy
Administrative policy framework
A person/s engaged under a contract
Australian Public Servant employee
Commander
Defence
Defence civilian
Defence locally engaged employee
Defence member
Defence personnel
Framework documents
Manager
Period of effect
Personal information
Policy domain
Policy owner
Provision
Sensitive information
Supervisor

For the purpose of this Policy, the following additional definitions apply:

Commentary Anything serving to illustrate a point; comment.

Communication A process that conveys shared meaning between individuals or between organisations and individuals.

Content Information contained in any communication, whether in audio, text, graphics, images etc.

Crisis

A crisis in Defence is an unplanned event, situation or matter of public concern that requires targeted attention, management, intervention or response beyond business-as-usual processes. A crisis is likely to occur quickly and has the potential to disrupt Defence's normal operations and activities. Crisis may undermine our reputation or challenge the public's sense of appropriateness, tradition, values, safety, security or the integrity of Defence. The focus of Defence's crisis communication efforts is to quickly and effectively address stakeholders, minimise physical and reputational damage, and return to normal business.

Defence installation

As defined in the *Defence Act 1903*.

Defence spokespeople

Defence spokespeople are those authorised to speak on behalf of Defence. They are a subject matter expert for the topic of the media engagement, who voluntarily agree to speak on behalf of Defence.

Embedded MECC communication team

Communication teams that are part of Ministerial and Executive Coordination and Communication (MECC) Division, who are embedded within each Group and Service.

Endorsement

Endorsement occurs when the Department of Defence provides its support publicly to an external party (such as an organisation, including charitable and not-for-profit organisations; private company; defence industry; individual; product, including publications; service; event or activity etc.) that may, or may not, result in a commercial benefit.

An endorsement may encompass verbal or written statements, such as a testimonial; imagery of Defence personnel, equipment or facilities; Defence logos; or any other characteristic that may lead people to believe there is an association between Defence and an external party.

Entertainment and non-news project

Entertainment and non-news projects include, but are not limited to:

a. television and radio programs (including participation in reality programs and competitions), scripts, short films, feature films, documentaries;

b. corporate videos, music videos, podcasts, blogs and artworks;

c. written products such as songs, poems and books (novels, textbooks, children’s literature etc.);

d. community service announcements and other such projects.

External party

Such as another government entity; organisation, including charitable and not-for-profit organisations; private company; defence industry; individual; event or activity organiser etc.

Imagery

Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media (such as still frame image files, motion video tape or files, hardcopy photographs etc.).

Intranet

An internet protocol (IP) network belonging to an organisation, usually a corporation, and accessible only to organisation members, employees etc., or people authorised by them.

Issue

An issue in Defence is an event, situation or matter of public concern that emerges over a period of time or is of a less-severe nature than a crisis. It could be an unfolding situation where the details are not yet known, or a persistent situation that remains of concern over a period of time. It is possible that a benign situation, or an issue, could turn into a crisis as the situation escalates, intensifies or broadens. The focus of Defence issues management is the same as crisis communication, with less urgent timeframes and, while communication planning may be proactive, Defence may take a reactive rather than a proactive posture for media engagement.

Media

A publication or broadcast program that provides news and feature stories to the public through various distribution channels such as newspapers, magazines, radio, television or online.

Military public affairs officer

Defence members who deliver Joint, Service-specific, operational, exercise and regional media and communication effects.

Official content

All content released by Defence is considered official.

Official Defence social media account

Any social media account that uses Department of Defence resources or is operated by Defence personnel in a manner that could be reasonably considered as representing the department, the Australian Defence Force (ADF) or their Groups or Services.

Public affairs guidance

Drafted by a public affairs officer to support operational incident reporting by providing a recommended public information approach.

Public comment

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, Defence media releases, contractor media releases and website testimonials, media responses, interviews, podcasts, background briefings, informal briefings, documents, letters to the editor, opinion pieces, articles, journals, academic/educational/research papers, public briefings, speeches, lectures, presentations, seminars, workshops, conferences, commentary, imagery, audio, internet sites, mobile networks and self-contained works.

Publications

Hard copy or soft copy documents intended for, or likely to be made available to the public, State authorities or foreign countries by way of free issue or sale. They include books and booklets (monographs or serials, hardback or paper bound), periodicals, journals, departmental and committee reports, instructional handbooks and manuals, posters and display material, binders for documents published in loose-leaf format, broadsheets, pamphlets, folders, leaflets, forms of advertising and business cards.

Public information

Text, audio or imagery content that has been cleared for public release or comment.

Regional manager for public affairs

Ministerial and Executive Coordination and Communication Division has a team of out-posted Regional Managers for Public Affairs (RMPA) who work collaboratively across Australia. RMPAs foster and maintain relations with local media and other key stakeholders. RMPAs work with Defence Establishment leadership, military public affairs personnel and others in the coordination of proactive engagement, media enquiries, issues, incidents, operations and events in their region.

Responsible officer

An SES Band 2 or 2-Star officer in the relevant Group or Service who is accountable for the content of an official Defence social media account and its adherence to this Policy.

Social media

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: social media networking sites (e.g. Facebook, Twitter, LinkedIn, SnapChat etc.); social review sites (e.g. Yelp, Tripadvisor, Goodreads, Google Reviews etc.); image-sharing sites (e.g. Instagram, Flickr, Pinterest etc.); video-hosting and live-streaming sites (e.g. YouTube, TikTok, Zoom, Skype etc.); community blogs (e.g. WordPress, Tumblr, Blogger etc.); discussion sites and professional military education websites (e.g. Whirlpool, Quora, Reddit, The Cove, Forge etc.); messenger sites (e.g. Messenger, Signal, WhatsApp etc.); collaborative sites (e.g. Wikipedia etc.); and dating sites (e.g. Tinder, RSVP, Bumble etc.).

Unofficial social media account

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.

Websites

A set of related webpages located under a single domain name. Are external to the department.

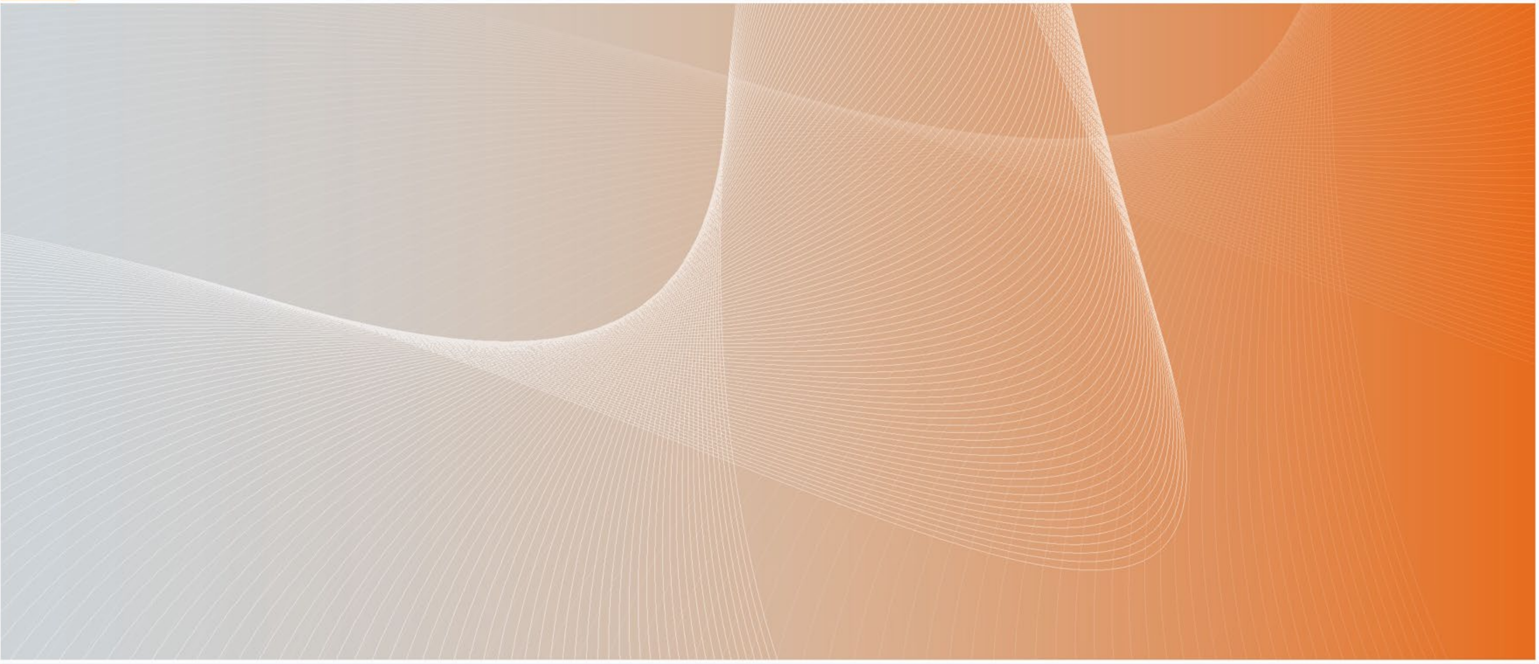
Australian Government
Defence

Social Media Playbook

Defence Social Media Hub

As at January 2023

(Note document is not controlled if printed)



Contents

Introducing the Social Media Playbook

Why is this Playbook important?

The Social Media Playbook is designed to support current Defence personnel inclusive of APS, ADF members and contractors who are responsible for an approved social media account.

This Playbook does not survey all social networks. Instead, it focuses on the most important networks to Defence and the Services. It offers best-practice information to consider before opening an account and when maintaining an account. The Social Media Playbook should be used in conjunction with the Defence Media and Communication Policy and Defence Media and Communication Guide.

This playbook will:

- Ensure greater alignment, consistency and a One Defence approach
- Maximise efficiency by providing best practice and examples
- Drive a strong social media presence and create trust

What you need to do:

Social media teams across Defence must continue to work to mitigate the risks associated with social media. This is why all areas and individuals seeking to establish a social media or digital communication presence must contact the Social Media Hub for advice prior to undertaking steps to do so. Requests should be flagged as early as possible to the Social Media Hub.

Please use this Playbook as a go-to resource for expertise and best practice. This playbook will be updated on a regular basis to keep up with latest platform trends.

Feedback is welcome and can be directed to the Social Media Hub.

Before opening a social media account

Defence personnel must consider the following sections before opening a social media account.

These are the foundations and planning tools to ensure your account aligns with Defence. Ultimately you/the social media account will be representing Defence; therefore, these sections need to be front of mind.

Social media policy

Defence personnel responsible for an approved Defence social media account must be familiar with the following Defence and Commonwealth policies:

❑ Defence Media and Communication Policy is the policy for the use of social media by Defence personnel.

❑ Defence Records Management Policy Operational Guide provides guidance on Defence's responsibilities in the management of Defence records in order to comply with Commonwealth legislation such as the *Archives Act 1983*; *Freedom of Information Act 1982*; *Public Performance, Governance and Accountability Act 2013*.

❑ DEF (AUST) GEO 7100 and 7101 (Parts A and B) are Defence policy on collection, classification and naming conventions for handheld and motion imagery.

❑ Defence Web Estate Manual is policy on Defence intranet, internet and extranet sites regardless of where they are hosted or by who. This includes defence.gov.au, ForceNET and social media sites where Defence has an account.

❑ Australian Government Branding are the guidelines on the use of the Australian Government logo by Australian Government Departments and Agencies.

❑ 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 Social Media Guidance is the current guidance on making public comment and participating online (social media).

❑ Copyright Act 1968 is the act which relates to copyright and the protection of certain performances, and for other purposes.

❑ Crimes Act 1914 is the act which relates to offences against the Commonwealth.

❑ Criminal Code Act 1995 is the act relating to criminal law.

❑ Defence Act 1903 is the acting relating to the provision of Military Defence and Protection of the Commonwealth and of the several states.

❑ Defence corporate identity style guide is a guide for web professionals on the requirements and details of the Defence web standards. It is strongly advised that only personnel with experience in the web design and development space should be using this framework.

❑ 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).

- ❑ Military Personnel Policy Manual The Military Personnel Policy Manual (MILPERSMAN) is designed to provide Defence personnel - and where it is a term of their contract - contractors, consultants and outsourced service providers with a primary source document for non-financial personnel policy advice and guidance.

- ❑ Privacy Act 1988 is an Act to make provision to protect the privacy of individuals and for related purposes.

- ❑ Public Governance, Performance and Accountability Act 2013 is an act about the governance, performance and accountability of, and the use and management of public resources by, the Commonwealth, Commonwealth entities and Commonwealth companies and for related purposes.

- ❑ Public Interest Disclosure Act 2013 is an Act to facilitate disclosure and investigation of wrongdoing and maladministration in the Commonwealth public sector, and for other purposes.

- ❑ Public Service Act 1999 is an Act to provide for the establishment and management of the Australian public service, and for other purposes.

- ❑ Statement of Ministerial Standards The ethical standards required of Ministers in Australia's system of government.

- ❑ Trade Marks Act 1995 is an Act relating to trademarks.

- ❑ Work Health and Safety Act 2011 is an Act relating to work health and safety, and for related purposes.

- ❑ Use of messaging apps: As per CIOG's Defence Guide to Enable Remote Working, and in reference to official communications: “Only a standard phone call / Apple FaceTime or Audio / Signal app can be used. As the above options provide a solution to all personal mobile phones as well as Defence issued phones, there is no need to conduct voice communications on any other applications such as WhatsApp, Viber, and Facebook Messenger etc…”
  - ❑ The Guide also advises that if working on the DPN-level, CIOG encourages the use of DPN-level communication tools like Skype, VERA and ForceNet.
  - ❑ Any further enquiries on messaging apps should be addressed to CIOG or your group CIOG representative.

Your security online

Public comment

Everything you post on social media is a reflection of Defence. Publishing online is public comment, and use of digital channels in an official capacity must be consistent with the values and strategic messages of Defence. This is why all areas and individuals seeking to establish a social media or digital communication presence must contact the Social Media Hub for advice prior to undertaking steps to do so.

It is essential that you do not post anything that could be seen to damage the reputation of Defence.

Maintaining security for Defence operations

If you have any doubt regarding operational security, you must seek appropriate guidance and clarification prior to making material public.

Who should you follow as an official account?

At your discretion, follow/connect with official and verified (blue tick) stakeholders who are of influence in your environment.

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 so be cautious about how much 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.

Social media for Defence leaders

In today's hyper-connected, social media age, social media is used by leaders across government and business to engage and communicate with audiences.

If you choose to have a social media account as a Defence leader, ultimately you are accountable for resourcing the account and adhering to the applicable governance of social media accounts.

As a leader within Defence with a social media account, it is your role to ensure communication through social media is aligned with the nature of your position is effective, compliant and aligned with Defence's strategic communications narrative. You, or your team managing the official social media account will be more effective with planned, proactive and structured messaging, rather than ad hoc.

It is not appropriate to use your rank, job or responsibilities to promote yourself through social media for personal or financial gain.

Some of the benefits to our senior leaders using social media are:

- Communicate directly with your audience
- Quick way to inform about emerging situations
- Stay relevant and guide change
- Share knowledge and experience
- Connect with your people on a human level
- Bridge geographical divides
- Combat imposters with your verified account

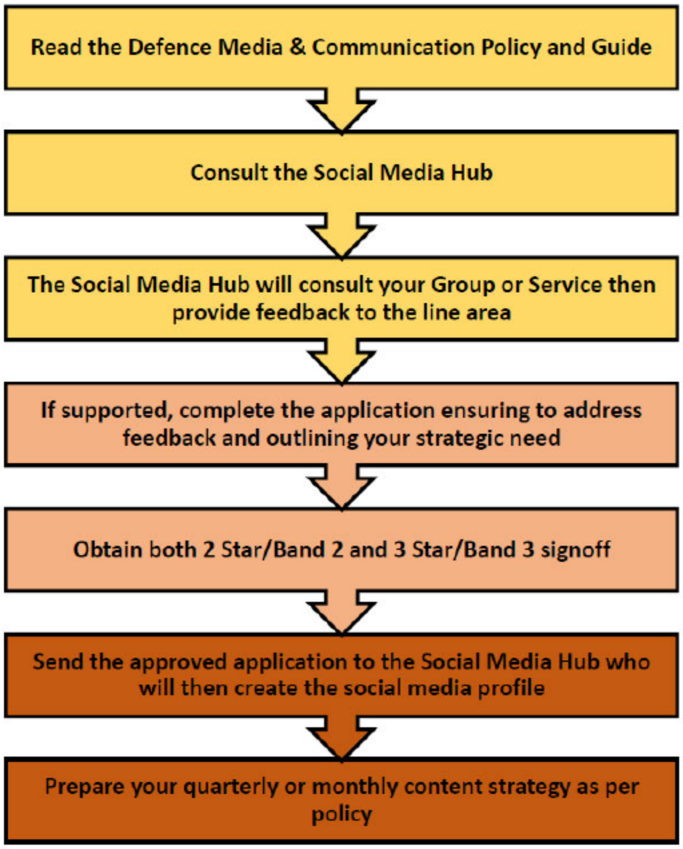
Social media for account managers/practitioners

As a social media account manager/practitioner, you are in charge of managing an official social media presence. Official accounts are those that have been created and approved by MECC and are managed using departmental resources including time, personnel and resources to communicate the work of the department.

All publicly available information, including social media content, must be cleared by a SES Band One or a One Star before release, however in some instances social media account managers might have Chain of Command authorisation to post on an official Defence social media account.

Business Application process

This is the official account application process and should be considered and completed before opening a social media account.



Read the Defence Media & Communication Policy and Guide

Consult the Social Media Hub

The Social Media Hub will consult your Group or Service then provide feedback to the line area

If supported, complete the application ensuring to address feedback and outlining your strategic need

Obtain both 2 Star/Band 2 and 3 Star/Band 3 signoff

Send the approved application to the Social Media Hub who will then create the social media profile

Prepare your quarterly or monthly content strategy as per policy

Requirements for each social media account

The requirements for organisational and positional accounts are:

	Organisational accounts	Positional accounts
Strategy and purpose	Each social media account needs to have a defined strategy and purpose.	Each social media account needs to have a defined strategy and purpose. Position-based accounts are professional, not personal. However, it is not mandatory for leaders to have accounts.
Approval and governance	There must be a formal governance and approval structure in place for the content and the profile. There must be a clear succession path and back up resources for when key people leave the team.	Accounts must be approved by MECC and relevant ADF HQ 3*/ Band 3. Formal approval processes do not apply if the account owner is posting the content. However, if a member of staff is posting on

	Accounts must be approved by MECC and relevant ADF HQ 3*/ Band 3.	their behalf they must gain approval from the account owner.
Archiving	Each account must be supported by a suitable archiving system that aligns with policy and legislation.	Each account must be supported by a suitable archiving system that aligns with policy and legislation.
Training	All personnel who have access to an approved social media account must take part in social media practitioner training provided by the Defence Social Media Hub.	Owners of individual accounts will be required to take part in social media practitioner training provided by the Defence Social Media Hub.
Process	Clear processes for using official social media must be adhered to including monitoring, approvals and responding.	Clear processes for using official social media must be adhered to including monitoring, approvals and responding. The handover of accounts on position changes must include password change, change of profile picture and notification to followers.
Content	Each profile must remain active, which requires a minimum of two posts per week. If this is not achievable then the account may be deemed as inactive. The goal is for all Defence social media accounts to have a common look and feel.	Each profile must remain active, which requires a minimum of two posts per week. If this is not achievable then the account may be deemed as inactive. The goal is for all Defence social media accounts to have a common look and feel.

Are you ready to have a social media account?

Before you commit to setting up a social media account, you need to carefully consider these aspects and discuss the viability of an account with your leaders/colleagues.

- ❏ Have you consulted the Defence Social Media Hub, your service's social media team, your embedded communications team or your functional command public affairs officer about the best social media platform to meet your intent?
- ❏ Have you undertaken an initial risk assessment covering hazards and controls of the use of social media (include risks associated with reputation; operational security; inappropriate and unacceptable behaviour; inappropriate data management; copyright violations; untrained content managers, content moderation, etc.)?
- ❏ Is there another social media profile that you could publish your content on? How do you distribute your content now?
- ❏ Have you read the relevant legislation and policy relating to social media?
- ❏ Have you completed the necessary social media training? If not, does your team have budget to fund initial and ongoing social media training?
- ❏ Does your team have the resources (tools, software, internet connection, budget etc.) to manage the account?
- ❏ Do you have the time required to open an account?
- ❏ Do you have the time required to monitor and community manage the account?
- ❏ Have you identified the purpose, desired end state and target audience of your proposed social media account?
- ❏ Do you have content sources and a content plan? What function will your content serve?
- ❏ How many posts per day can you manage? Will this sustain your audience or will the account become dormant?
- ❏ Do you have budget to provide the resources, training, devices and infrastructure to build and scale this account?

Setting up your social media account

Requesting a social media account

All social media accounts are required to be registered with the Defence Social Media Hub and your Service or Group headquarters as per the Defence Media and Communication Policy. The registration of a social media account is a formal process and all information relating to the registration must be kept on record and stored in Objective.

To request a new social media account, there is a formal process that requires both MECC Social Media Hub involvement and 3*/Band 3 line area approval. Information and a process map on the approval process is available on the Social Media Hub's Intranet page.

Setting up an official social media account

Setting up your social media account takes time and requires design work for profile images and header images. To ensure a consistent and professional approach across Defence social media accounts, each page must have a similar look and feel and be aligned with Defence branding and follow the guidelines provided below.

Account security

You should not create shared user logons to manage official accounts, where it is a breach of the platform's terms of use to do so, as the accounts may be deactivated if detected. Under the terms of use for Facebook and LinkedIn, administrators are required to use their real personal Profiles to manage official Pages. LinkedIn settings and Facebook Business Manager ensure there is a clear and separate interface between the personal and official.

Passwords to official accounts should be changed regularly and specifically when there are staff changes to minimise the risk of deliberate or unintentional misuse. Other simple procedures to preserve the integrity of accounts include:

- Passwords should comply with Defence policy. They should be complex, no shorter than nine characters, which contain digits, punctuation and special characters as well as letters.
- 2-factor authentication should be activated.
- Only log-on to the password-protected accounts when you need to post an official message and log off immediately afterwards.
- Do not use personal mobile devices to connect to official accounts for publishing. Account managers should use Defence issued devices.
- If an erroneous message is published accidentally, account managers should immediately advise their supervisor, and not attempt to correct or retract the message without seeking advice.

- The CyberSense video series is an educational tool for Australian Government agencies which also informs staff about information security threats. Refer to www.cyber.gov.au/advice for information.

Name of the page/account

This is the name that will appear when users search for a page. Additionally, this is the name that will appear in the post when you are tagged by other accounts.

For naming conventions, contact Social Media Hub or relevant Service level brand manager.

Handle/username

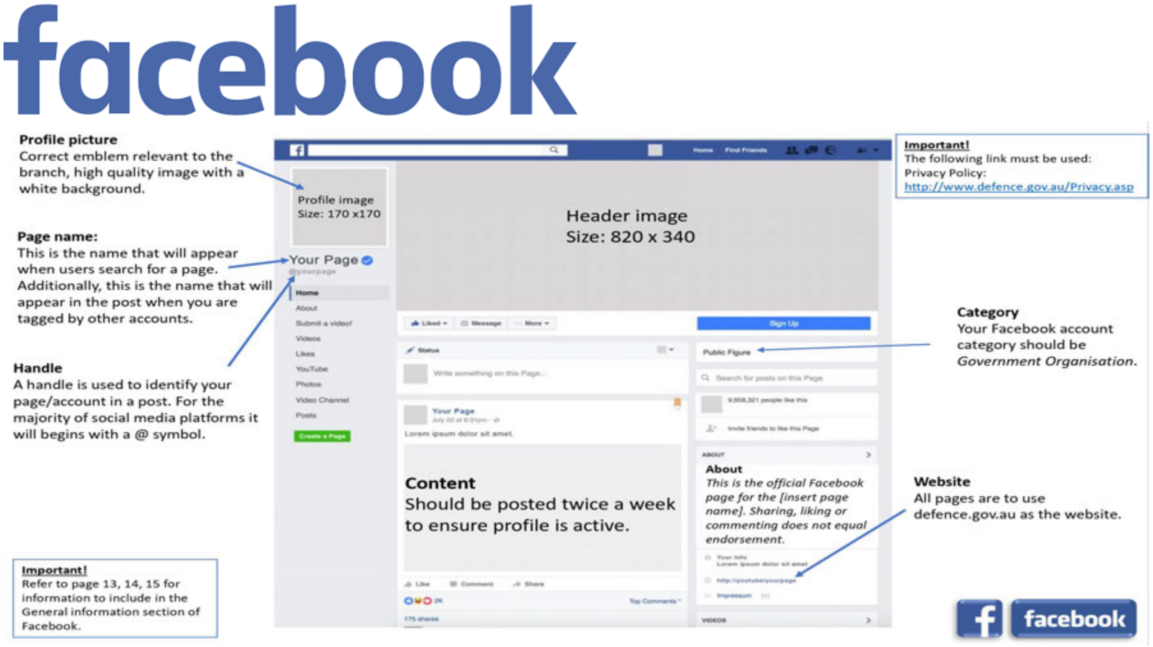
A handle/username is used to identify your page/account in a post. For the majority of social media platforms it will begins with an @ symbol.

Your account's handle should be the same on all social media (i.e. Twitter, Instagram, and Facebook). Having a handle that is the same on every platform makes it easier for people to find you. Keep in mind that there is a limit of 15 characters on Twitter.

For handle/username conventions, contact Social Media Hub or relevant Service level brand manager.

Note: The Social Media Hub may assist you with setting up your new approved social media account.

Facebook



Profile picture
Correct emblem relevant to the branch, high quality image with a white background.

Page name:
This is the name that will appear when users search for a page. Additionally, this is the name that will appear in the post when you are tagged by other accounts.

Handle
A handle is used to identify your page/account in a post. For the majority of social media platforms it will begins with a @ symbol.

Important!
Refer to page 13, 14, 15 for information to include in the General information section of Facebook.

Profile image
Size: 170 x170

Header image
Size: 820 x 340

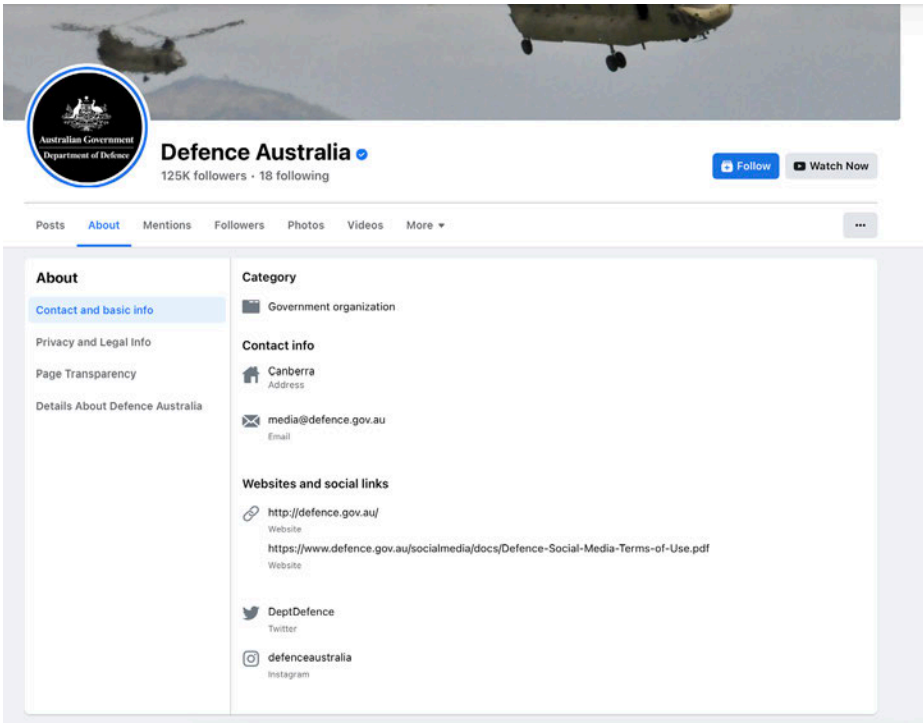
Content
Should be posted twice a week to ensure profile is active.

About
This is the official Facebook page for the [insert page name]. Sharing, liking or commenting does not equal endorsement.

Important!
The following link must be used:
Privacy Policy:
http://www.defence.gov.au/Privacy.asp

Category
Your Facebook account category should be *Government Organisation.*

Website
All pages are to use defence.gov.au as the website.



Defence Australia
125K followers · 18 following

About

Contact and basic info

Privacy and Legal Info

Page Transparency

Details About Defence Australia

Category

Government organization

Contact info

Canberra
Address

media@defence.gov.au
Email

Websites and social links

http://defence.gov.au/
Website

https://www.defence.gov.au/socialmedia/docs/Defence-Social-Media-Terms-of-Use.pdf
Website

DeptDefence
Twitter

defenceaustralia
Instagram

Other Facebook details

Page/account profile pictures

Your Facebook profile's picture should be:

- The official emblem relevant to the branch and of good quality
- Adhere to the relevant branding guidelines (e.g. white background)
- Designed to 170x170 pixels.

About section - Facebook

This is the official Facebook page for the [insert page name]. Sharing, liking or commenting does not equal endorsement. For Defence Social Media Terms of Use refer: defence.gov.au/socialmedia/docs/Defence-Social-Media-Terms-of-Use.pdf

Category
Your Facebook account category should be Government Organisation.

Founded
Use 1942 when the Department of Defence was founded, or alternatively when the relative service was founded.

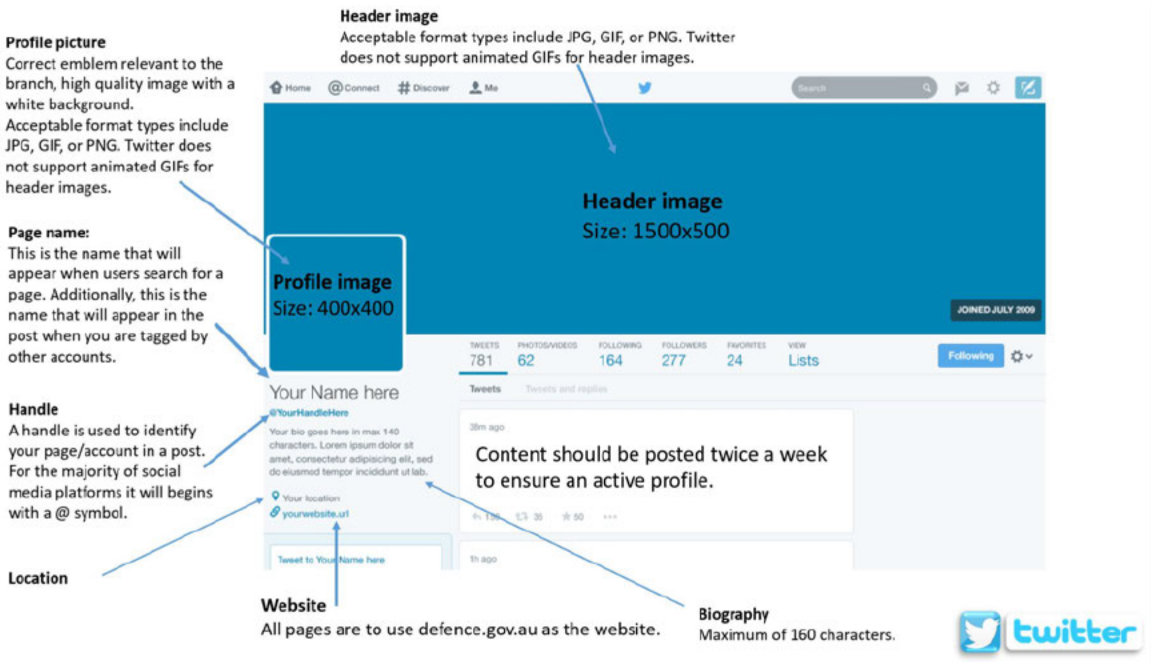
Business type
Tick 'This Page represents a corporate office or headquarters'.

Phone number
The only phone number to be used is the Defence national switchboard number 1300 333 362. This should never be the personal or business number of the page manager or any other member of Defence.

Email address
This is to be a @defence.gov.au email address however should not be a name of any Defence personnel. If you do not have a generic Defence email address, speak with the Social Media Hub.

Website
All pages are to use defence.gov.au or relevant service as the website.

X



Profile picture
Correct emblem relevant to the branch, high quality image with a white background.
Acceptable format types include JPG, GIF, or PNG. Twitter does not support animated GIFs for header images.

Page name:
This is the name that will appear when users search for a page. Additionally, this is the name that will appear in the post when you are tagged by other accounts.

Handle
A handle is used to identify your page/account in a post. For the majority of social media platforms it will begins with a @ symbol.

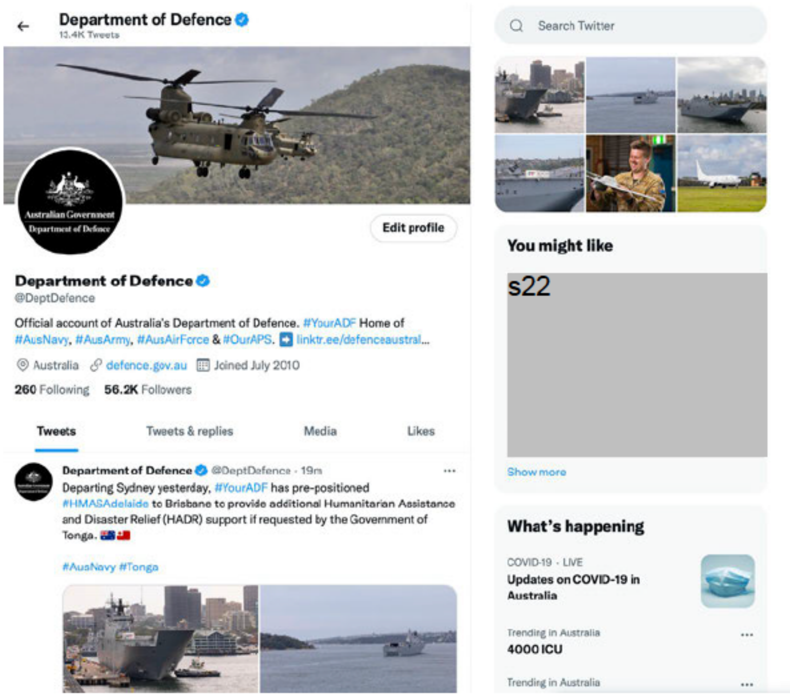
Location

Header image
Acceptable format types include JPG, GIF, or PNG. Twitter does not support animated GIFs for header images.

Content should be posted twice a week to ensure an active profile.

Website
All pages are to use defence.gov.au as the website.

Biography
Maximum of 160 characters.



Department of Defence
13.4K Tweets

Search Twitter

Edit profile

Department of Defence
@DeptDefence

Official account of Australia's Department of Defence. #YourADF Home of #AusNavy, #AusArmy, #AusAirForce & #OurAPS. ➡ linktr.ee/defenceaustral...

Australia defence.gov.au Joined July 2010

260 Following 56.2K Followers

Tweets | Tweets & replies | Media | Likes

Department of Defence @DeptDefence · 19m
Departing Sydney yesterday, #YourADF has pre-positioned #HMASAdelaide to Brisbane to provide additional Humanitarian Assistance and Disaster Relief (HADR) support if requested by the Government of Tonga. 🇦🇺🇹🇴

#AusNavy #Tonga

You might like

s22

Show more

What's happening

COVID-19 · LIVE
Updates on COVID-19 in Australia

Trending in Australia
4000 ICU

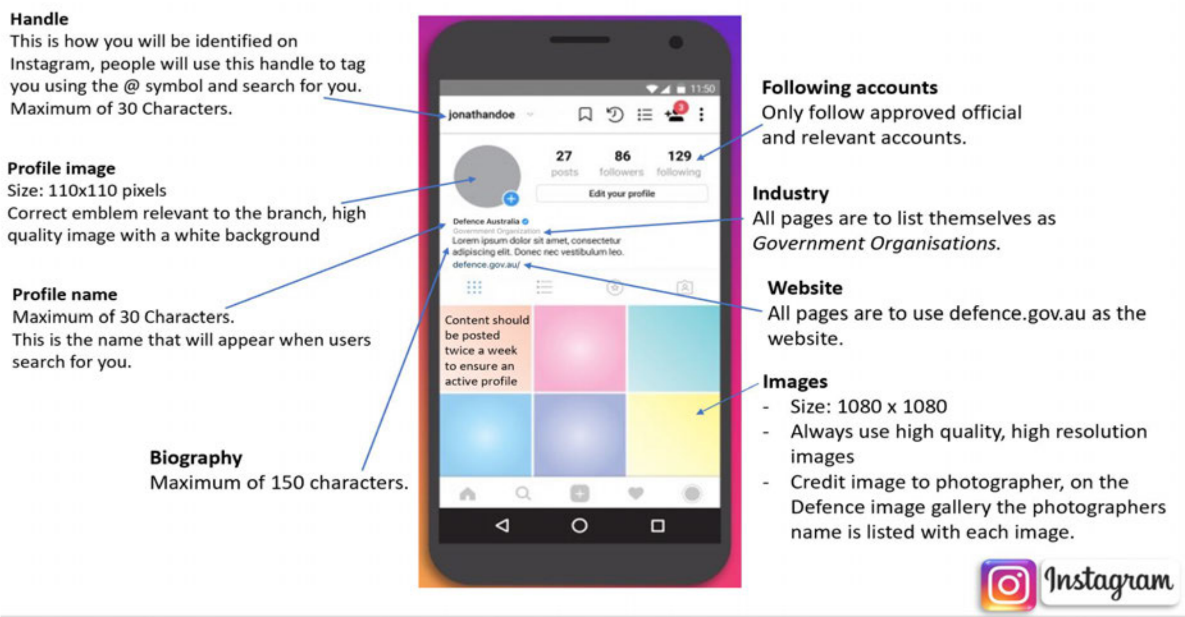
Trending in Australia

Your X profile checklist:

- ❑ Header photo (recommended dimensions are 1500x500 pixels). Photos can be in any of the following formats: JPG, GIF, or PNG. Twitter does not support animated GIFs for header images.

- □ Profile photo (recommended dimensions are 400x400 pixels). Photos can be in any of the following formats: JPG, GIF, or PNG. Twitter does not support animated GIFs for profile images.
- □ Bio (maximum 160 characters) about the account
- □ Location.
- □ Website must be specified.

Instagram



Handle
This is how you will be identified on Instagram, people will use this handle to tag you using the @ symbol and search for you. Maximum of 30 Characters.

Profile image
Size: 110x110 pixels
Correct emblem relevant to the branch, high quality image with a white background

Profile name
Maximum of 30 Characters.
This is the name that will appear when users search for you.

Biography
Maximum of 150 characters.

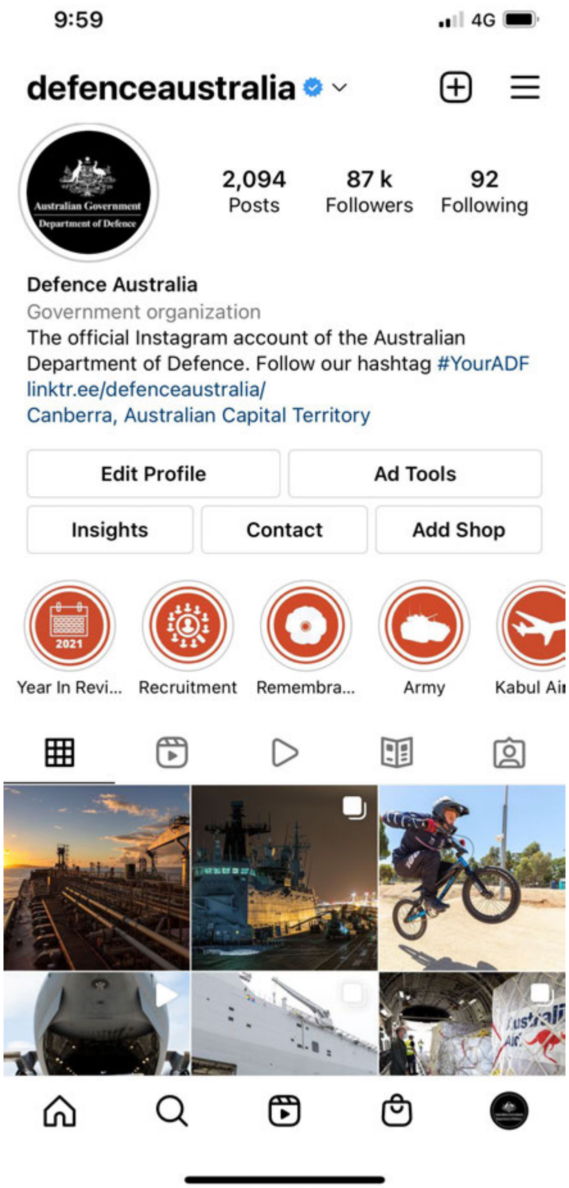
Content should be posted twice a week to ensure an active profile

Following accounts
Only follow approved official and relevant accounts.

Industry
All pages are to list themselves as *Government Organisations.*

Website
All pages are to use defence.gov.au as the website.

Images
- Size: 1080 x 1080
- Always use high quality, high resolution images
- Credit image to photographer, on the Defence image gallery the photographers name is listed with each image.



defenceaustralia

2,094 Posts · 87 k Followers · 92 Following

Defence Australia
Government organization
The official Instagram account of the Australian Department of Defence. Follow our hashtag #YourADF
linktr.ee/defenceaustralia/
Canberra, Australian Capital Territory

Your Instagram profile checklist:

- ❏ Profile photo (recommended dimensions are 110x100 pixels). Photos can be in any of the following formats: JPG, GIF, or PNG. Instagram does not support animated GIFs for profile images.
- ❏ Bio (maximum 150 characters) about the account
- ❏ Handle with @ symbol. Needs to be max 30 characters
- ❏ Industry needs to be Government Organisation
- ❏ Website needs to be defence.gov.au

Ongoing support for your social media account

Once you have set up your account, you will need to continually monitor your account for the following:

Securing the operational account

Digital security is more important than ever.

It's important you keep your new account 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 and make sure your critical accounts have strong passwords.
- ❏ Limit administrative privileges to only Defence personnel who need access in order to do their job.
- ❏ Regularly audit the administrators and managers of accounts to ensure only those who need access retain it.
- ❏ Log out whenever a profile isn't in use.
- ❏ Administrators and managers must be made 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.
- ❏ 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.

Managing your account

Moderation/Community Management

Moderation is the manual or automatic process for assessing and removing social media material (including images, comments/replies etc.) that goes against the Defence Social Media Terms of Use.

To ensure a positive experience for users, you should ensure that all public commentary is appropriate and moderated correctly during business hours.

It's 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.

Some social media platforms like Facebook automatically moderate for basic breaches, such as the use of profanities, however, it is best practice to update the custom word list to block a wider range of profane words.

Platform guides to build a custom word list:

- Facebook
- Instagram
- YouTube
- X: Non available
- LinkedIn: None available, self-moderation required

The Defence Social Media Terms of Use should be posted to each of your accounts 'About' section so that your audience are aware of what behaviour is acceptable and what is not. You may also block or delete users if they have breached the Defence Social Media Terms of Use.

Additional resources:

- Incident Response Decision Matrix
- Reporting of Offensive content Matrix

Standard Operating Procedures on moderation or community management best practices are available here.

Social Media profile handover guide

Whether you've stepped into a new role, are consolidating pages, or taking on another positional account, chances are you'll need to handover your social media accounts at some point. Every social media platform has a different process when it comes to handing over accounts.

Handover checklist:

- **Email address/s**

Provide access to the email address (usually a shared inbox) to the incoming operator.

- **Login and Passwords for all accounts**

Provide the login details for all social media accounts to the incoming operator. Ensure these are provided in a secure manner.

- **Provide social media training**

Ensure that the incoming operator has undertaken social media training to prepare them for the job particularly if they are operating multiple profiles. They need to be prepared to handle all situations including incidents, trolls and spam.

- **Provide brand compliance training**

Ensure the incoming operator is across the brand standards and values. This is important when producing content and representing the brand online. This includes the correct logo, profile image, header image, keeping the about section up to date, ensuring content and messaging aligns with the brand and its purpose.

- **Provide content training**

Ensure the incoming operator is across the style of content that the page produces this includes: types of images, style of writing and key messaging to align with the brand. They also need to be across how frequently they should be posting on each and when.

- **Explain any tips and tricks**

This could include tips for increasing engagement, getting posts approved, best times to post for particular topics, topics or types of posts to avoid etc. Big events coming up that the page usually covers and may require planning in advance.

- **Introduce to key contact people**

Including: People from the Social Media Hub, other services and groups, digital media, newspapers, media and any other relevant groups. Ensure they are added to any email lists for relevant meetings and reports.

- **Provide tools – phones, laptops, access to required software**

Ensure that the incoming operator has the tools to conduct their job this includes a smartphone, laptop and/or tablet.

- **Resource requirements**

Evaluate if the incoming operator requires additional resources in the team. This could be the case that they have another role in addition to running the social media and may require support or a back-up operator to assist them during busy periods.

- **Inform users of the operational change**

PAO, Command and HQ need to know who the point of contact is.

- **Hand over admin rights and brand manager access to HQ**

Handing over admin rights to HQ

Facebook

Page:

Only the admin of the page can assign someone else as an admin. If you are only an editor you do not have this privilege and you will need to contact the admin to do this. Keep in mind that they must accept your invite before they can start to manage your page.

1. Click **settings** at the top of your page.
2. Click **page roles** in the left column
3. Type a name or email in the box and select the person from the list that appears.
4. Click **Editor** to select a role from the dropdown menu
5. Click **Add** and enter your password to confirm

If you need to change someone's role from editor to admin:

1. Click **settings** at the top of the page
2. Click **page roles** in the left column
3. Click **edit** next to the name of the person whose role you want to change and then select a new role from the dropdown menu
4. Click **save**. You may need to enter your password to confirm.

Group:

Group members must visit the group in order to be made an admin. Keep in mind that when you make someone an admin they will be able to make changes to the group including, adding or removing members, editing content.

1. From your newsfeed, click **groups** in the left menu and select your group
2. Click **members** in the left menu
3. Click the next to the person you want to make an admin or moderator.
4. Select **make admin** or **make moderator.**

Business manager access:

Make sure the partner you send the link to is an admin of the business page. Once you share the link they must open this link within 30 days or it will expire. The link may only be used once.

1. Go to Business Settings.
2. Click **People**.
3. Click **Add**.
4. Enter the work email address of the person you want to add.
5. Select the role you'd like to assign them. Be sure to read the description for each role. Choose either **Employee access** or **Admin access**. You can also select **Show Advanced Options** to choose **Finance analyst** or **Finance editor**.
6. Click **Next**.
7. Select the asset and the task access you want to assign the person.
8. Click **Invite**.

Instagram

If you'd like someone to be able to boost on your Instagram business account, there are three ways to give them the appropriate permissions:

1. Edit Page roles. If you own the Page that is connected to your business's Instagram account, you can give other people permission to post or boost your business.

2. Add people to your Business Manager. If you're using Business Manager to manage Page roles, you'll need to assign roles in Business Manager.
3. Add people to your ad account. Adding people to your advertising account doesn't give them permissions to log in as you or see things on your profile that you haven't shared with them.

   Or provide the user name and password to the relevant person in HQ. Ensure they are notified of any future password changes.

X

1. Click "Add access".
2. Enter their handle.
3. Choose the access level you want to grant them from the drop-down menu.
4. If you're choosing Account administrator or Ads manager, you will also have the option to turn on "Can compose promotable Tweets".
5. Click "Save changes".

Or provide the relevant username and password to HQ. Ensure they are notified of any future password changes.

Handing over a positional account

Positional accounts will need to be handed over when they leave particular positions for example: Chief of Defence Force, Vice Chief of Defence Force, Chief of Army, Chief of Navy, Air Chief Marshall etc.

1. Download an archive of the page
2. Upload the archive to objective.
3. Handover all associated username, password and email address details.
4. Change the name of the page (if the name includes the name of the previous person).
5. Request to change the handle (if it mentioned the name of the previous person).
6. Change the profile image to an official portrait image of the incoming person.
7. Change the header image if required.
8. Change the description (if it mentions the previous person who held that position).

Facebook

Download an archive of your page:

If you're an admin, you can download a copy of your Page. The file includes:

- Posts, photos and videos shared on the Page by people who work on the Page.
- A list of people who have roles on the Page.
- A description of the Page's current settings.
- Page info from the About section.

To:

1. Click **Settings** at the top of your Page.
2. From **General**, click **Download Page**.
3. Click **Download Page**.
4. Click **Get Started**, then click **Start Downloading**.

When the file is ready, you'll receive an email or a notification, depending on your privacy settings. From the email or notification, click **Download Page** and enter your password to continue. Keep in mind that the link to your file will expire after 4 days.

Change page name:

You'll need to be an admin to request a change to your Page's name.

To request a change to your Page's name:

1. Click **About** on the left side of your Page.
2. Click **Edit** next to your Page's name.
3. Enter a new Page name and click **Continue**.
4. Review your request and click **Request Change**.

Change handle/username:

You'll need to be an admin to change your Page's username. If you're an admin:

1. Click **About** on the left side of your Page.
2. Click **Edit** next to your current Page username.
3. Enter a new username.
4. If the username is available and follows the guidelines for custom usernames, click **Create Username**.

Note: Changing of handles/username can potentially be denied by the platform if the account has already been verified.

X

Download an archive of your page:

1. Go to your **Account settings** by clicking on the **profile** icon at the top right of the page and selecting **Settings and privacy** from the drop-down menu.
2. Under **Your Account**, click **Download an archive of your data.** It will ask you to enter your password.
3. When your download is ready, we'll send a notice via push notification (if you have Twitter for iOS or Android installed on your mobile device). From your settings, you can click the **Download archive** button under the **Download your data** section.

Change your username/handle:

Your username can be up to 15 characters long.

1. Click on **Settings and privacy** from your **profile** icon dropdown menu.
2. Under **Your Account**, click on Account Information. It will ask you to enter your password.
3. Click on **Username.** Update the username currently listed in the username field. If the username is taken, you'll be prompted to choose another one.
4. Click the **Save changes** button.

Note: Changing of handles/username can potentially be denied by the platform if the account has already been verified.

Change your display name:

Your display name can be up to 50 characters long.

1. Click on **Edit profile** on the right-hand side, below the header image.
2. Under your profile picture you can edit the display name in the top box.
3. Click save on the top right-hand side.

Instagram

Download an archive of your page:

If you want a copy of everything you've shared on Instagram, you can request a download of your data in a machine readable (JSON) format. You'll need your Instagram account password to request this information.

From Instagram on the Web:

1. Go to your profile and click **Settings**
2. Click **Security**
3. Scroll down to **Data Download** and click **Request Download**
4. Enter the email address where you'd like to receive a link to your data and enter your Instagram account password
5. You'll soon receive an email titled **Your Instagram Data** with a link to your data. Click **Download Data** and follow the instructions to finish downloading your information.

From iOS or Android:

1. Go to your profile and tap
2. Tap **Settings**
3. Scroll down and tap **Data Download**
4. Tap **Request Download**
5. Enter the email address where you'd like to receive a link to your data and tap **Request Download**
6. Enter your Instagram account password
7. You'll soon receive an email titled **Your Instagram Data** with a link to your data. Click **Download Data** and follow the instructions to finish downloading your information.

Note: It may take up to 48 hours for us to email you a download link. Some data you have deleted may be stored temporarily for safety and security purposes, but will not appear when you access or download your data.

Change your handle and username:

To update your profile information, including your username and email address associated with your account:

1. Go to your profile
2. Tap **Edit Profile** or **Edit Your Profile**
3. Type in your information and tap **Done** (iPhone) or ✓ (Android) in the top right

Note: Changing of handles/username can potentially be denied by the platform if the account has already been verified.

How to hand over an organisational account

If you operate an organisational account when you leave your position you will need to hand over to the new operator.

1. Add a new admin to the page if you are the current admin. On Facebook only the admin can make certain changes and if you are the only admin and no longer involved this could hinder the operation of the page.
2. Hand over all usernames, passwords and email account details to the incoming operator.
3. Introduce the incoming operator to any relevant contacts for this position e.g. Media, social media hub, digital media.
4. Handover any branding and content material to ensure that the page continues to align with the correct branding and messaging. Provide training if necessary.
5. Provide or organise training for social media to prepare them for the job ahead particularly if they are running multiple profiles and using unfamiliar software to do so.
6. Provide tools e.g. Phone, laptop, tablet, access to software.
7. Provide content training and share any tips and tricks regarding content e.g. What material works/does not work, topics to avoid, correct messaging, safe pages to share or tag.
8. Ensure there are enough resources to operate and monitor the pages, evaluate if more resources are required.
9. Inform users of operational change e.g. PAO, Command and HQ.
10. Ensure HQ has access to all pages.

Social Media Archiving

Australian Government departments/agencies are accountable for their actions and decisions on social media. Hence when using social media for business activities, Defence must keep accurate and sufficient information documenting these activities.

This information needs to be kept in a usable and accessible form for as long as it is needed.

The Archives Act 1983 does not limit the definition of information and records by their format. Business information created as a result of using social media is subject to the same business and legislative requirements as business information created by other means.

Which social media interactions to keep?

A monthly record of all social media posts that have been published on Defence owned social media accounts should be downloaded and saved in Objective. The download is to include engagements such as comments as well.

Different information has different value and purpose. More valuable social media information, such as policy feedback, announcements or complaints, needs to be retained appropriately.

What about third-party sites?

When using third-party social platforms, you must ensure that you meet any Australian Government obligations, including the management of information.

Social media records held in their native applications on third-party sites may not be legally regarded as a Commonwealth record[1]. Despite being created by an Australian Government department/agency, the information may not be able to be retained or accessed over the long term. Therefore it is important to capture records at regular intervals.

How to capture records at regular intervals?

The processes below allow you to capture multiple records at regular intervals (for example, weekly, fortnightly, or monthly) as part of a business process.

Download directly from the platform

- Use the export or download feature of the social media platform or messaging app. You can select a particular date range, type of information (for example, posts, photos and videos, messages) or different file formats for download.
- The downloaded file should be captured into your agency's records management system. Data may be downloaded as a CSV, Excel or HTML file from a social media account and saved locally to an official PC before being captured into the system.

Capturing and storing social media content

Facebook: https://www.facebook.com/help/466076673571942

- From your News Feed, click **Pages** in the left menu.
- Go to your Page.
- Click **Settings** at the top of your Page.
- From **General**, click **Download Page**.
- Click **Download Page**.
- Click **Create File**.

X: https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive

- Go to your Account settings by clicking on the more icon in the navigation bar, and selecting Your account from the menu.

[1] https://www.naa.gov.au/information-management/types-information-and-systems/types-information/managing-social-media

- Click on Download an archive of your data.
- Enter your password under Download an archive of your data, then click Confirm.
- Verify your identity by clicking Send code to your email address and/or phone number on file. If you do not have an email address or phone number on file, you will be redirected to the Account information page.
- Enter the code sent to your email address and/or phone number.
- After verifying your identity, click the Request data button. If your Twitter account is connected to Periscope, you'll have the option to request an archive of your Periscope data on Periscope directly.
- When your download is ready, we'll send an email to your connected email account or a push notification if you have the app installed. From your settings, you can click the Download data button under the Download data section.
- Once you receive the email, click the Download button while logged in to your Twitter account and download a .zip file of your Twitter archive.
- Save to Objective.

Instagram: https://help.instagram.com/contact/505535973176353

- Go to Settings and click on 'Privacy and Security'. Once there, you'll find 'Data Download' towards the bottom of the list.
- If you select 'Request Download' from here, you'll be able to leave an email address where you'll be notified once the data has been prepared. Instagram says that it can take up to 48 hours for the information to become ready for download, but it typically takes much less time than that.
- When the information is ready, you'll receive an email that directs you back to the same section under 'Privacy and Security'. From here, you'll be able to download the data directly to your computer in a single ZIP file.
- Save to Objective.

After you download the archive of your profile, you are required to upload this to Objective in line with the Freedom of information Act.

If you require additional guidance on how to do this, contact your supervisor for Objective training or refer to the Objective one-stop shop on the Defence intranet, at
s47E(d)

How to delete your social media account

Follow below steps to delete your chosen platform. Once the account is closed, please inform the Social Media Hub via s47E(d) @defence.gov.au of the following details:

- Account name
- Account URL
- Date of closure.

Facebook

https://www.facebook.com/help/223786757631885

To delete your Page, you'll need to be an admin of that Page. If you're an admin:

1. From your News Feed, click Pages in the left menu.
2. Go to your Page and click ⚙ Page Settings in the bottom left.
3. From General, click Remove Page.
4. Click Delete [Page name].
5. Click Delete Page and then click OK.

Keep in mind that when you request we delete your Facebook Page, Facebook will unpublish your Page immediately but it won't be permanently deleted until 14 days have passed. You can also unpublish your Page at any time.

Instagram

https://help.instagram.com/370452623149242

Before deleting your account, you may want to log in and download a copy of your information (like your photos and posts) from Instagram. After your account has been deleted, you will not have access to Instagram’s Data Download tool.

1. Go to the Delete Your Account page from a mobile browser or computer. If you're not logged into Instagram on the web, you'll be asked to log in first. You can't delete your account from within the Instagram app.
2. Select an option from the dropdown menu next to Why are you deleting your account? and re-enter your password. The option to permanently delete your account will only appear after you've selected a reason from the menu.
3. Click or tap Delete [username].

LinkedIn

https://www.linkedin.com/help/linkedin/answer/131147

LinkedIn Page super admins can deactivate their Page for a company or school, or Showcase Page.

Ensure your Page meets all necessary criteria before deactivating. Additionally, review the result of deactivating your Page.

Deactivate your LinkedIn Page or Showcase Page:

1. Access your Page Super admin view.
2. Click the Admin Tools dropdown and select Deactivate Page or Deactivate Showcase Page.
3. Click the checkbox to confirm the implications of deactivating the Page.

4. Click Deactivate.

You'll see a confirmation window that your Page has been successfully deactivated. If the Page can't be deactivated, you'll receive an error message.

X

https://help.twitter.com/en/managing-your-account/how-to-deactivate-twitter-account#deleting-your-twitter

For up to 30 days after deactivation it is still possible to restore your Twitter account if it was accidentally or wrongfully deactivated.

1. Click on Settings and privacy from the drop-down menu under your profile icon.
2. From the Account tab, click on Deactivate your account at the bottom of the page.
3. Read the account deactivation information, then click Deactivate @username.
4. Enter your password when prompted and confirm that you want to proceed by clicking the Deactivate account button.

After your 30-day deactivation window, your Twitter account is permanently deleted. When you don't log into your account during the 30-day window, it lets Twitter know you want to permanently delete your Twitter account. Once your account is deleted, your account is no longer available in their systems. You won't be able to reactivate your previous account and you won't have access to any old Tweets.

YouTube

https://support.google.com/youtube/answer/55759?hl=en#zippy=%2Cdelete-your-channel-permanently

Closing your YouTube channel will permanently delete your content, including videos, comments, messages, playlists, and history. Note that you can't currently delete a channel on mobile devices.

1. Sign in to YouTube Studio.
2. From the left sidebar, select Settings .
3. Select Channel › Advanced Settings.
4. At the bottom, select Remove YouTube Content. If you're asked to, enter your sign-in details.
5. Select I want to permanently delete my content.
6. Select the boxes to confirm you want to delete your channel.
7. Select Delete my content.

It may take some time for your channel to be permanently deleted. In the short term, you may continue to see thumbnails of your videos on the site.

Note: These steps will only delete your YouTube channel, not your Google Account you use to sign in with. Learn how to delete your entire Google Account.

After you delete a channel, the channel URL and channel name will no longer be visible or searchable in YouTube Analytics. Data associated with the channel, such as watch time, will still be part of aggregate reports, but will not be attributed to the deleted channel.

Content guidelines

Respecting intellectual property

You should not publish any copyrighted or trademarked material without the authorisation of the copyright or trademark owner.

This includes embedding a song, or linking to unattributed artwork, using popular songs as background to a video.

In the event you use copyrighted content, the owner of that content may bring action for an infringement of the copyright. The relief a court may grant includes an injunction and either damages or an account of profit. The court may award damages in order to deter similar infringements of copyright.

You should only use approved images, as found/available on the Defence Image or Video Gallery.

Refer to this checklist before you post:

- ❑ Have you advised all content providers that copyright of content posted to social media created by Defence members will and does belong to the Commonwealth?
- ❑ Have you advised all content providers that all text and imagery must have associated data with it in order to comply with the policy and legislation? For example, photos must have metadata applied or stored with it and it must be stored in a content management system such as Objective?
- ❑ Have you advised content providers that posts must not violate copyright? For example, posting non-Defence imagery or videos containing commercial music without the owner's permission is a violation of copyright?
- ❑ Have you advised all content providers that posts must not use the badges and symbols of the ADF or the individual services without authorisation?

Creating content

Social media should be used to tell a story and create a conversation about what Defence and the services are doing, has done and will do in the future.

Aligning content with the Defence values

During content planning, consider how your copy and image/s or video aligns with Defence or your Services values. These specific Defence values provide a common and unifying thread for people working in Defence and for the public to understand what unites Defence.

The Defence values are:

- **Service:** The selflessness of character to place the security and interests of our nation and its people ahead of my own.
- **Courage:** The strength of character to say and so the right thing, always, especially in the face of adversity.
- **Respect:** The humanity of character to value others and treat them with dignity.
- **Integrity:** The consistency of character to align my thoughts, words and actions to do what is right.
- **Excellence:** The willingness of character to strive each day to be the best I can be, both professionally and personally.

Aligning content with your service or group values

Refer to your service or group's values and ensure your content aligns with their values.

Suggested content types

- Turn a Defence news article into a post
- Live videos
- 360 photos or videos
- Infographics
- Poll your audience
- Find interesting statistics to make into a post
- Add emoji or symbols
- Media releases
- Share or retweet from other pages
- Videos with subtitles
- Stories
- Live videos

Writing for social media

Always consider your audience when preparing content for social media. Defence and the services has its own terminology, acronyms and abbreviations however these are unlikely to be understood by the public.

Everything you write for social should promote Defence and your services strategic messages which summarise who we are, what we do and why we do it. Strategic messages are a guide used across our organisation in all communications based in these key themes:

- ADF
- APS
- Capability
- Services: Army, Air Force, Navy
- Community and family
- Health and welfare
- Personnel and employment
- Veterans
- History and commemorations
- Industry
- Technology

Writing for social media is different to any other way of writing. It requires you to be innovative, informative, relaxed, simple, memorable, fun and align with Defence and your Service's strategic communication narrative all at once.

Additionally, each platform requires a different style of writing. You need to think about why people go to the platform - to find information, to connect, socialise, and to catch up on what the people they know are doing. You should aim to make posts as engaging as possible.

Acronyms and abbreviations

The public does not understand Defence or Service acronyms, abbreviations and other shortened forms. An exception may be justifiable for particularly complicated terms if the use of an acronym or other shortened form will significantly reduce repetition.

Capitalisation

Defence personnel have a tendency to over-capitalise words. Words are not capitalised because the writer considers the word important. Words are capitalised because they are proper nouns or proper/official names.

Headings must use minimal capitalisation. Only the first word and any proper nouns are to be capitalised. Do not use uppercase for Exercise names. Example: it should be 'Exercise Bersama Gold' and not 'EXERCISE BERSAMA GOLD'.

Hashtags

Hashtags are words or phrases preceded by the # hash symbol. They are quick way to label content for search functionality and join a conversation. They are also great ways to gather content so people can follow topics, trends and events of interest.

How do we use them?

- Hashtags are required to be 'all one word' meaning they will break if there are any spaces between words, or if the # symbol is missing from the beginning.
- They can be used to abbreviate long phrases such as TYFYS which stands for Thank You For Your Service and TBT – Throwback Thursday. As users become familiar with your content and hashtags, so too will their understanding of these acronyms.
- To create a new one, simply start using it in posts and click on them regularly to view the results as they can be hijacked easily.
- Become familiar with popular hashtags such as #DYK meaning Did You Know, as some are used widely across different platforms.
- To save on characters and remove the need for unnecessary words, search for or create hashtags that can be built directly into the copy. For example, '#YourADF has begun Operation X'.
- Don't use hashtags that are too common like #And for #The, the results for these are too broad and will not look appealing your audience.
- Keep hashtags short; long hashtags, also known as CamelCase can make hashtags comprising of two or more words easier to read, however the shorter you can make it, the more memorable and successful its use will be.

A large list of commonly used Defence hashtags and tags can be found on the Social Media Hub Intranet page: s47E(d) [redacted]

Tagging

Tags allow social media users to engage an individual, business or any entity with a social profile when they mention them in a post or comment. Tags are sometimes referred to as @mentions and can be used by simply typing the desired account handle preceded by the @ symbol.

Like hashtags, account handles, and therefore tags, need to be kept as 'all one word' without any spaces. Tagged accounts will receive a notification, or a 'heads up' that you've tagged them and may decide to share or reply to content as a result. If used correctly, tags can make a big difference to how your post performs.

If you have a number of accounts to tag on Twitter and cannot fit them within the character limit, tag them within the image instead. Keep in mind, for business pages, all account tags are public and can been seen by any user and make sure you are tagging the correct account.

Emoji

An emoji is a visual representation of an emotion, object or symbol and provides a quick shortcut to expressing or communicating a message, description or feeling. Emoji's can be used to complement a message, or be used in place of words to reduce a character count.
The use of emoji's may not be appropriate for all situations and a degree of judgement should be exercised when using them for delicate subjects such as commemorations or memorial services.

For example, the use of a poppy might be appropriate, whereas a tank or explosion emoji is not. A good tip is to scan similar profiles or consult with a colleague for a second opinion if you aren't too sure.

Keep in mind that too many emoji's can easily distort a message or distract a user from your message's intent. It's important to keep yourself aware and up-to-date with an emoji's meaning as seemingly innocent emoji's can sometimes represent something completely different.

Writing checklist

❑ **Listen:** before you can talk to your audience you have to understand and embrace how they talk about you. Your community should inform your voice and your content (to an extent). Language should be kept formal however the use of appropriate emoji and more colloquial terms is accepted. Understanding you audience personas are key to increasing engagement.

❑ **Don't react:** Although social media is fast paced, there is time to ensure that each post is compliant, educated and aligns with strategy.

❑ **Write to one action:** you want your fans to 'like', share, comment or click your link. Determine what action you're trying to get your community to do—what action are you trying to spur? If there's more than one thing, it can get too confusing. Keep it simple as comment below to show support for… or ask questions which encourages comments.

❑ **Writing standards still apply:** It is important to ensure correct grammar and spelling is used for all content and comments. It is recommended that all posts are put through a word template or through a spelling and grammar check to assist with this. If you do make an edit on social media you do have the option to edit it on all platforms except Twitter. For Twitter, we would recommend taking the post down and correcting the mistake and reposting if you are able to do so in a timely manner.

❑ **Experiment, measure, and respond:** be innovative with your posts, but ensure you use metrics to understand what works for your audience. If something doesn't work you can adjust for next time. Find what works, but also have some variety to ensure you are keeping up with trends.

❏ **You're only as good as your next post:** when it comes to writing for any social platform, you can't rest on laurels. After every post that falls flat and after every successful post, you should ask, "How can I make this better?"

❏ **Don't just share a post:** if you are sharing a post make sure you post your own comment too. Also consider if it is right for your unit, brigade, formation or branch audience.

❏ **Keep it short:** with so much content on social media your audience's news feeds are crowded. Therefore, people are scrolling through and not engaging with the content. They will not often spend more than three seconds on a post. It is important that you capture their attention within the first 100 characters of your post.

❏ **Don't forget a high quality approved image or video:** the easiest way to capture your audience is to include a picture or video. Ensure that any image or video has been cleared and is taken from the Defence image and video Gallery.

❏ **Before you publish, consider:**
- ❏ Is the text too long?
- ❏ Is it engaging?
- ❏ Have you tagged other Defence, Services or verified Defence-related pages?
- ❏ Does it cover who, what, where, when, why and how?
- ❏ What is your hashtag strategy?
- ❏ Is there too much information?
- ❏ Does it align with the strategic narrative and the lines of effort?
- ❏ Has the photo or video been approved by a One Star and provided to Digital Media?
- ❏ Has the content been approved by a One Star or delegate?

Using images and video on social media

Using images and videos on social media increases engagement, reach, reaction, shares and comments. The more engaging the product, the more your post stands out.

The images and videos add meaning to your words. Additionally, they convey emotion, evoke a reaction and communicate messages.

With videos the shorter the better, with most followers only viewing maximum nine seconds of any video it is key that those nine seconds count.

You may use any image/video from the Defence image or video gallery.

Choosing the correct image is key, posting more than five images up on social media requires followers to take an extra step of clicking on an image to see more, which many will not do. Additionally, posting five images that say the same thing or feature the same personnel or capability will retract from the authentication of your post.

Images or videos checklist

- □ Confirm the product has been cleared by MECC/strategic centre and is published in the Defence Image Library or Defence Video Portal (as these products have already been cleared, have metadata applied and are archived in an approved storage system).
- □ Collate and apply generic metadata to images and place in an appropriate folder (archive folder) on an approved records management system.
- □ The product has been provided to Digital Media. All products must be submitted with metadata to s47E(d) @defence.gov.au.
- □ Operational security is maintained by checking the setting for confidential information.
- □ Product reflects Defence and your services values and professionalism.
- □ Product reflects correct WHS and COVID safe standards.
- □ Uniforms need to be of good repair and worn correctly.
- □ Product reflects good weapon handling/control (i.e. weapons are not to be pointed at people unless in combat or realistic training scenarios). Civilians are not to be depicted handling weapons.
- □ Product with corporate promotional material is not to be associated with any alcohol or tobacco related merchandise or any dubious corporate identity.
- □ Product including children must have parental consent obtained (and included in metadata). Only children's first names (or an alias/nom de plume) are to be given in the caption/mid-caption to protect the child's identity from exploitation.
- □ Product with vehicles can show civilians in the driver's seat, but images must also show a supervising Defence member and the vehicle must be obviously stationary.
- □ Do not digitally alter a photo or video.

What can go wrong?

When social media content is not approved by MECC/the strategic centre, your copy and imagery/video can have a severe impact on global situations. It is crucial you consider the nature of content and how it impacts current relationships, operations, and exercises. You should always explore the ramifications of posting content before it's published.

Reputational damage can be amplified by social media, and negative media coverage can quickly go viral. Screen captures by the public, of deleted content can sometimes attract more attention than if the post were to be kept live.

Before sharing any content on any social media platform, it's important to read/view content in its entirety before hitting share. This includes videos and image galleries. Don't assume what the content may be due to a title/description.

Content Approval

After drafting your social media post and have selected an approved image or video, your content needs to be cleared by your 2 Star/Band 2 officer or their delegate.

When choosing an approved image, look closely to make sure the image does not display any small details, like Defence access passes, or information written on whiteboards for example. 9 times out of 10, these issues are identified, however it's always best to double check these before your posts go live. Once approved, your content can then be posted or scheduled for an appropriate time.

For information on gaining clearance for an image or video that you or your team have sourced locally, refer to Chapter 9 of the Media and Communications Policy.

Best times to post on social media

Is there really a best time to post on social media? Always.

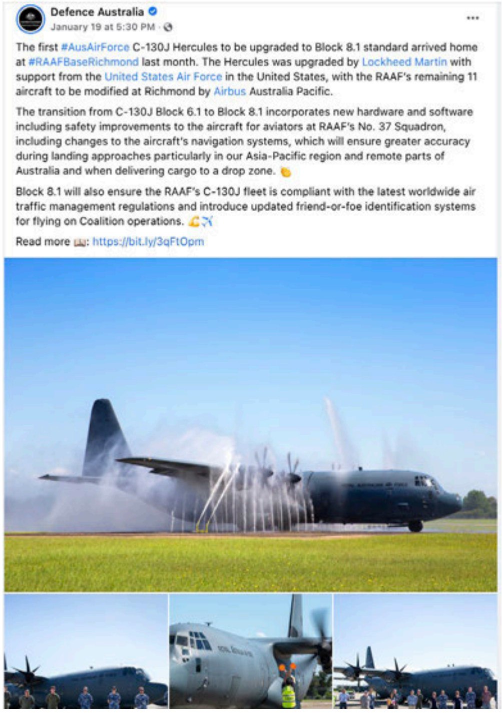
The key challenge is in rising above the noise and getting eyes on your posts. It is important to consider that algorithms are increasingly moving away from the reverse chronological timelines and towards relevance-based curation.

The best way to ascertain your ideal slots, is to get into the backend of each of your platforms to see when your audience is online and adjust accordingly..

Examples of good content

What makes this post good?

- Correct hashtags used
- Correct page used
- Short link used
- Striking images from Defence Image Gallery used
- Relevant/engaging content used



Defence Australia
January 19 at 5:30 PM ·

The first #AusAirForce C-130J Hercules to be upgraded to Block 8.1 standard arrived home at #RAAFBaseRichmond last month. The Hercules was upgraded by Lockheed Martin with support from the United States Air Force in the United States, with the RAAF's remaining 11 aircraft to be modified at Richmond by Airbus Australia Pacific.

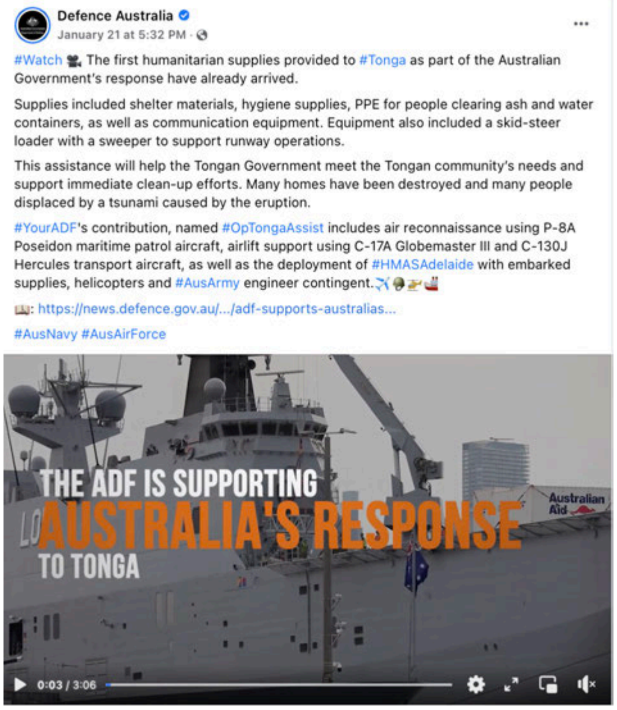
The transition from C-130J Block 6.1 to Block 8.1 incorporates new hardware and software including safety improvements to the aircraft for aviators at RAAF's No. 37 Squadron, including changes to the aircraft's navigation systems, which will ensure greater accuracy during landing approaches particularly in our Asia-Pacific region and remote parts of Australia and when delivering cargo to a drop zone. 👏

Block 8.1 will also ensure the RAAF's C-130J fleet is compliant with the latest worldwide air traffic management regulations and introduce updated friend-or-foe identification systems for flying on Coalition operations. 💪✈️

Read more 📖: https://bit.ly/3qFtOpm

What makes this post good?

- Call to action to watch the video
- Video from the Defence video gallery used
- Brief description of what the video is about
- Video renamed to title, rather than edit file name, e.g. V0001defencevdieo
- Engaging cover image used



Defence Australia
January 21 at 5:32 PM ·

#Watch 📽️ The first humanitarian supplies provided to #Tonga as part of the Australian Government's response have already arrived.

Supplies included shelter materials, hygiene supplies, PPE for people clearing ash and water containers, as well as communication equipment. Equipment also included a skid-steer loader with a sweeper to support runway operations.

This assistance will help the Tongan Government meet the Tongan community's needs and support immediate clean-up efforts. Many homes have been destroyed and many people displaced by a tsunami caused by the eruption.

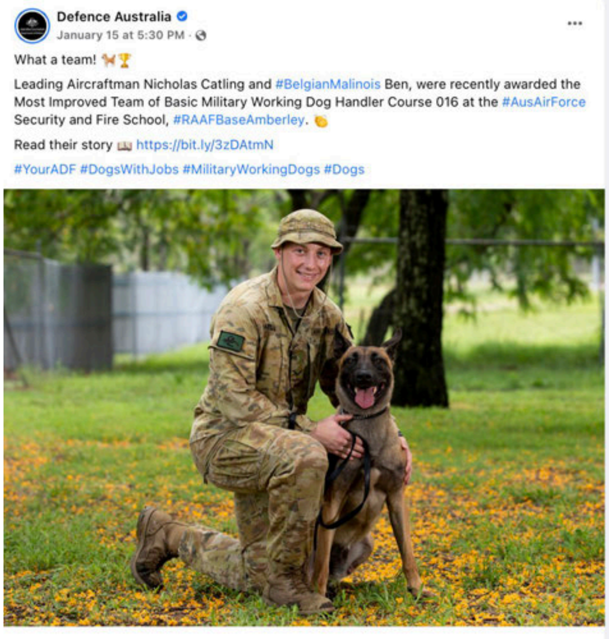
#YourADF's contribution, named #OpTongaAssist includes air reconnaissance using P-8A Poseidon maritime patrol aircraft, airlift support using C-17A Globemaster III and C-130J Hercules transport aircraft, as well as the deployment of #HMASAdelaide with embarked supplies, helicopters and #AusArmy engineer contingent.✈️🪖🚁🚢

📖: https://news.defence.gov.au/.../adf-supports-australias...

#AusNavy #AusAirForce

What makes this post good?

- Call to action to 'Our People' tab on Defence News website
- Image from Defence Image Gallery used
- Concise summary of story with key points to gain audience used
- Appropriate emoji used
- Information and messaging from a cleared PAG used



Defence Australia
January 15 at 5:30 PM ·

What a team! 🐕🏆

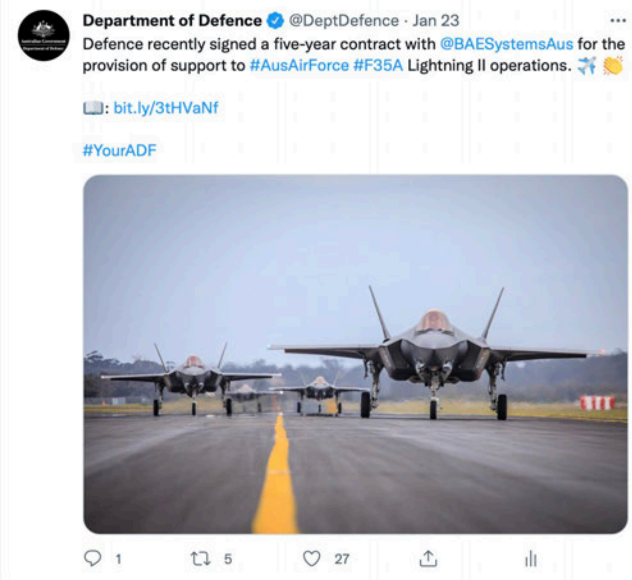
Leading Aircraftman Nicholas Catling and #BelgianMalinois Ben, were recently awarded the Most Improved Team of Basic Military Working Dog Handler Course 016 at the #AusAirForce Security and Fire School, #RAAFBaseAmberley. 👏

Read their story 📖 https://bit.ly/3zDAtmN

#YourADF #DogsWithJobs #MilitaryWorkingDogs #Dogs

What makes this post good?

- Hashtags used
- Correct pages/accounts used
- Short link used to Defence News story
- Image used from Defence Image Gallery



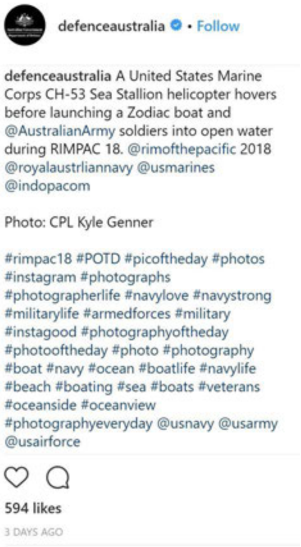
Department of Defence @DeptDefence · Jan 23

Defence recently signed a five-year contract with @BAESystemsAus for the provision of support to #AusAirForce #F35A Lightning II operations. ✈️👏

📖: bit.ly/3tHVaNf

#YourADF

Good content examples



defenceaustralia • Follow

defenceaustralia A United States Marine Corps CH-53 Sea Stallion helicopter hovers before launching a Zodiac boat and @AustralianArmy soldiers into open water during RIMPAC 18. @rimofthepacific 2018 @royalaustrliannavy @usmarines @indopacom

Photo: CPL Kyle Genner

#rimpac18 #POTD #picoftheday #photos #instagram #photographs #photographerlife #navylove #navystrong #militarylife #armedforces #military #instagood #photographyoftheday #photooftheday #photo #photography #boat #navy #ocean #boatlife #navylife #beach #boating #sea #boats #veterans #oceanside #oceanview #photographyeveryday @usnavy @usarmy @usairforce

594 likes

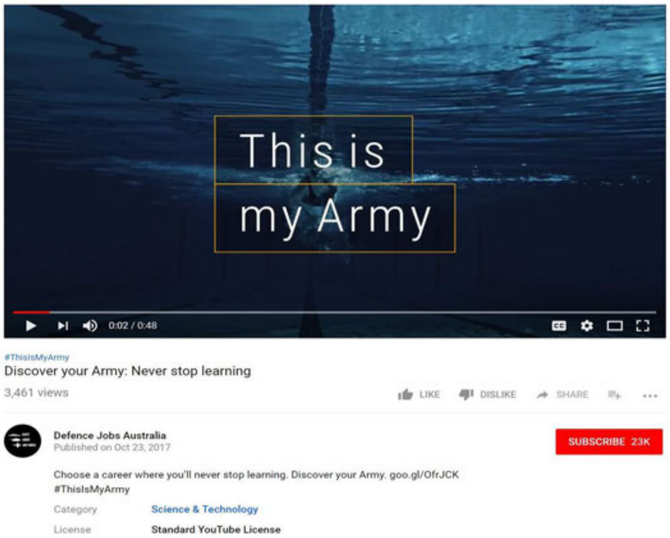
3 DAYS AGO

What makes this post good?

- Quality image from the Defence image gallery
- White border added for consistency across the profile and to ensure the whole image fits within Instagram's sizing requirements
- Hashtags used to increase engagement
- Relevant pages tagged
- Short concise caption used to describe the image
- Photographer credited

Instagram

Good content examples



#ThisIsMyArmy

Discover your Army: Never stop learning

3,461 views

Defence Jobs Australia
Published on Oct 23, 2017

Choose a career where you'll never stop learning. Discover your Army. goo.gl/OfrJCK
#ThisIsMyArmy

Category	Science & Technology
License	Standard YouTube License

What makes this post good?

- Short caption
- Relevant hashtag used
- High quality video
- Videos can also be found on the Defence Video Portal
- Description about video supplied
- Text overlay throughout video for people watching without sound
- Video organised into the correct category
- No copyrighted content used ie. Music, video, images

YouTube

Sharing content with the MECC Social Media Hub

If you have content that can be shared by Defence Australia or a service or group page and you don't have a social media account, follow this checklist before sending content to your relevant service or group or the Social Media Hub.

- ❏ When submitting photos or video, they must be cleared by your Band 1 or One Star equivalent and be made available on the Defence image/video gallery.
- ❏ Cleared photos and videos must include captions that cover the 5 W's: who, what, when, where and why
- ❏ Content should be written clearly, concisely and avoiding jargon
- ❏ Remember - tweets are limited to 280 characters, including spaces
- ❏ Content should have mass appeal
- ❏ Don't wait until the last minute. Plan your content and include social media in your planning process to allow adequate time for posts to be developed
- ❏ Send content to your relevant service or group or the Social Media Hub for consideration with the following information:
  - ❏ preferred posting date
  - ❏ message or angle
  - ❏ who to tag or mention
  - ❏ requested text, and
  - ❏ imagery or image gallery identity number with.

Using social media for crisis communication

Real-world incidents can be amplified by social media. Social media can help Defence to be transparent during a crisis however you and your Chain of Command need to agree on the strategy and approach before using social media to manage a crisis.

What to have in place in the event of a crisis:

❏ Identify the lead Government Department/Agency in charge during the crisis
❏ Coordinate a Defence social media team and establish responding protocols
❏ Ensure that lead Government Department/Agency is aware of your social media content before publishing any content
❏ Only post to Defence social media accounts once approvals are received
❏ Ensure that everyone knows who to alert in each scenario
❏ Check fake news for situational awareness.

Refer to this checklist for guidance:

❏ Be prepared: during a crisis, ensure you thoroughly understand the severity of the issue/s and the associated risks to Defence. From here you need to make a call on whether you will use social media to engage with your audience or not. If you choose to engage, you should be able to preempt questions your audience will ask and draft responses to answer their questions. Approved talking points can assist in this scenario.

❏ Be prepared: to hold on all BAU social media posts. Scheduled posts will need be removed immediately to avoid any insensitivities that may transpire.

❏ Outline roles and responsibilities: it's vital everyone in your team knows what their role is during a crisis and commits to it, whether it's monitoring social media or providing up-to-date reports on the issue.

❏ Circulate and adhere to your escalation process: issues can spread quickly through social media so it's important to understand who to go to when you need to escalate something.

❏ Monitor: during the crisis, closely monitor the accounts and influencers talking about the issue. Be prepared to respond to them directly if necessary.

❏ Recovery: As the severity of the crisis loses traction on social media, you should prepare a report on how the issue was managed using social media and share your learnings with your peers.

❏ Prevention: post-crisis, look for opportunities to refine and improve existing processes and procedures based on what worked well and what didn't. Continue to monitor social media with the best possible situational awareness.

Social media measurement and metrics

Your social media strategy should outline what you want to achieve for each social media account. To demonstrate the value of your work and to adequately report on how your social media content is performing, you need to know how to access and navigate, and understand and interpret social media analytics.

At its core, social media engagement is whenever someone interacts with your social media profile. It comes in the form of metrics including:
Likes
Follows
Shares
Comments
Retweets
Click-throughs

These metrics are crucial for measuring the effectiveness of your content or campaign.

Another factor involved in determining the effectiveness of your content are content signals. These include:

- How long a user spent watching a video - were video captions included?
- Did a user stop scrolling to read your content – was it written to capture attention quickly?
- What time the content was posted – was it during a peak period of activity for your audience?
- Did the user stop scrolling to comment or share your content – Did you ask the audience a question? Or was the content written with the intention of evoking an emotional response?

Understanding the analytics behind what content is and isn't working, allows you to adjust and make decisions during content planning. Establishing a benchmark engagement rate will allow you to identify if your content is performing well of your strategy requires a revision.

To understand why social media metrics matter, refer to our 'Resources' section on the Intranet.

Community Management

For inappropriate comments, a robust profanity filter is essential. The Defence Social Media Hub can supply you with one including terms specific to Defence. Comments deemed inappropriate should only ever be replied to once with approval. Users who continue to be inappropriate or disruptive after this can be managed by:

- Hiding, which allows you 'hide' inappropriate comments or posts from your audience. These can only then be seen by the original poster and their followers.

- Deleting, where a screenshot of the comment must first be taken before filing.
- Ban the user, if they they continually do not meet yours or the platform's community guidelines.

Mute is a feature that allows you to remove an account's Tweets from your timeline without unfollowing or blocking that account. **Muted** accounts will not know that you've **muted** them and you can unmute them at any time.

Analysing how your audience responds to different types of content will give you an idea of what response you are likely to receive for future content.

Negative or inappropriate comments can be categorized by three groups. These are:

- Category 1 – Borderline comments, including;
  - Offensive language,
  - Spam or material that isn't relevant
  - Comments directed at Defence or its leaders,
  - Criticism of other users and disrespectful exchanges.

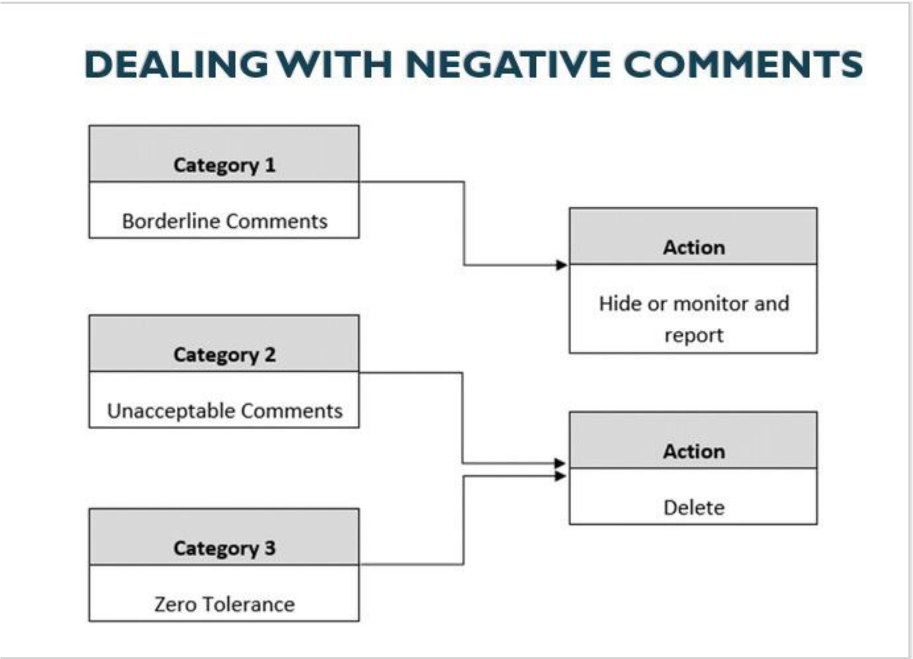
Category 2 – Unacceptable comments, including;

- Disrespectful behavior towards Defence and other users
- Uploading inappropriate images and GIFs, or using offensive terminology and language.
- Targeting comments directly at other users through tagging them.
- Encouraging or supporting illegal activities.
- Support of violent, extreme, or controlling behavior

Category 3 – Zero Tolerance comments, including;

- Blatantly disrespectful behavior
- Comments which incite, induce or aid hatred towards others.
- Comments that support or encourage violence
- Encouraging or supporting illegal activities or operations
- Comments which may incite, encourage or make reference to conduct that may constitute a serious criminal act

Use your own judgement when determining which category an unacceptable comment falls under and if you aren't sure, simply hide the comment.



DEALING WITH NEGATIVE COMMENTS

Category 1

Borderline Comments

Category 2

Unacceptable Comments

Category 3

Zero Tolerance

Action

Hide or monitor and report

Action

Delete

Users that publish comments within Category 1 – ‘Borderline’ should be warned, or politely reminded of the profile or platform’s community guidelines. Using judgement, hide or report the comment if necessary.

Users that publish comments within Category 2 and 3 may require a more stern approach involving one or more of the following actions:

- The user be warned, either through direct message or within the comment thread.
- The users comment, or comments, be screen captured and deleted.
- If persistent, all recent comments screen captured and the user banned from the profile.

All screenshots should be filed diligently within Objective.

Frequently asked questions

Do social media handles have to be consistent?

Yes. Consistent social media handles make it easier for your audience to find and tag you.

Do I have to have an account on every social media network?

No. You need to be strategic with the social media network you choose. An easy way to figure out which social media account you need is to consider where your audience is.

Another way to determine which social media network to choose is by considering the content people on each network want to see. For example, if you have the resources to make and clear videos, you should consider YouTube to share those videos.

What type of content should my account share?

Your social media content should align with what your audience wants to see. You can create or find relevant content they're likely to enjoy and share. The Defence News website and Defence YouTube channels should be your first port of call.

How often should I post?

Your posting frequency depends on your resources and audience. When you commit to a social media account, you should aim to deliver quality content to your audience. You should never sacrifice the quality of your social media content for quantity. As a guide, MECC Social Media Hub commits to a minimum 2 posts per day to maximise audience engagement.

What's the best time to post?

It depends on when your audience is most active across each social media network. Use the analytics from each network to identify which content gets the most engagement i.e. what time of the day, what day and what type of content has high engagement – this should be your foundation.

Should I use a social media content calendar?

Each social media account is required to develop a content plan for approval. The content plan should be developed between the senior social media and/or communications adviser with business team or service team.

Using a content calendar to coordinate and schedule social media content is best practice and recommended. The Social Media Hub currently uses Asana to plan its social media content**.**

Can I create a fake/dummy social media account for social media administration and/or monitoring purposes?

No. Defence personnel are not to create fake or dummy social media accounts for the administration of official organisational or official positional Defence Social Media accounts, or create accounts for the specific purpose of monitoring of Defence issues.

Social media accounts for administrative purposes

Facebook and LinkedIn pages require the connection of personal accounts for account administration. These accounts must be genuine user accounts and cannot be fake or dummy accounts as per relevant platform user policies:

- Facebook [Account integrity and authentic identity] – an account name must be the authentic name you go by in everyday life, and any personal account (as used for administrative purposes) must not be accessed by more than one person.
- LinkedIn [User Agreement] – users must use their real name on their profile and must not create a false identity on LinkedIn or misrepresent their identity.

Fake or dummy accounts detected by the platforms connected to official Defence Facebook or LinkedIn Defence accounts, may result in the platform limiting account access or removing both the user and official account.

Social media accounts to monitor Defence Issues

Defence or personal social media accounts are not be created for the specific purpose of monitoring Defence Issues[2]. Lines areas or individuals seeking to monitor Defence Issues in the public domain should contact their relevant embedded MECC Communication Officer for access to **Streem**, Defence's official media monitoring tool.

Furthermore, as defined in the Defence Media Communication Policy, [Annex A – Definitions, Official Defence social media account], any account that 'uses Defence resources or is operated by Defence personnel in a manner that could be reasonably considers as representing Defence, the Australian Defence Force or their Groups and Services' is considered an official account and must not be created without approval, as laid out in Defence Media and Communication Guide [Chapter 6, New Official Defence social media accounts].

As per Defence Media and Communication Guide [Chapter 6, Requirements for posting and interacting on Defence official social media accounts] in regard to the use of existing official Defence Social Media accounts, Defence personnel may be authorised to monitor other accounts

[2] [Defence Media Communication Policy, [Annex A – Definitions, Issue] *An issue in Defence* is *an event, situation or matter of public concern that emerges over a period of time or is of a less-severe nature than a crisis. It could be an unfolding situation where the details are not yet known, or a persistent situation that remains of concern over a period of time. It is possible that a benign situation, or an issue, could turn into a crisis as the situation escalates, intensifies or broadens. The focus of Defence issues management is the same as crisis communication, with less urgent timeframes and, while communication planning may be proactive*'.

where it relates to their duties and responsibilities and is in accordance with legislative and policy obligations.

For further advice or guidance, please contact the Defence Social Media Hub at s47E(d) @defence.gov.au

Other social media platform terms

- X [Deceptive identities] - If you are engaged in impersonation or are using a misleading or deceptive fake identity, the platform may permanently suspend your account.
- Instagram [Terms of Use] - You may not impersonate someone or something that you are not, and you cannot create an account for someone else unless you have their express permission.

Quick Reference Guide for hashtags

Hashtags vary by platform, with Twitter and Instagram being heavy users. Always search a platform for use and check appropriateness before adding to your content. Hashtags should 'add value' to your content, not simply be an add-on.

Refer to the document entitled 'Social Media Reference Guide to Tags and Hashtags' available under 'Resources' on the Intranet.

Quick Reference Guides - Setting up your page and using it

Set up your organisation Facebook page:

1. Click the home button next to your name
2. Click on the Pages tab in the explore section of the left-hand sidebar of your profile home page.
3. Click **create page**
4. Choose page type, *Government Organisation*
5. Name your page with the previously agreed naming convention
6. Upload a profile image by clicking on **add a picture** in the profile image area. Ensure you use a high quality 170x170 version of the official emblem relevant to the brand on a white background.
7. Upload a cover image by clicking on the **add a cover** link on the top left of cover image section. Ensure the cover image is high quality approved imagery relevant to the page the size should be 828 x 315.
8. Update the following sections with this information:

   Founded: 1942 or when the relevant organisation was founded
   Business type: This page represents a corporate office or headquarters
   Phone number: Defence national switchboard 1300 333 362
   Email: a defence email address that does not include personnel members name is to be used.
   Website: defence.gov.au
   General information: As above in the setup guide.

Using your account: How to post to your page

1. Click on the **make a post** box
2. Add any text you want to include
3. At the bottom you have the option of adding photos, videos etc.
4. Ensure relevant pages are tagged
5. Ensure relevant hashtags are used
6. If scheduling the post, ensure the date and time are correct.

7. If the post is not being scheduled click the blue **post** button on the bottom right of the post.
8. Your post has been posted to your page.

Using your account: How to share to your page

1. At the bottom right hand side of each post is an arrow with the word **share** underneath, click on this.
2. The option to **Share to a page** will pop up, click this.
3. If you are an administrator of the page through your personal account, ensure that the post will be shared to the organisations page and not your personal one.
4. If required, add an over quote to further clarify the post you are sharing.
5. If no text is required, click on the blue **share** button on the bottom right side.
6. The post has been shared to your page.

Quick Tips:

- ❏ Don’t spam your followers
- ❏ Tag other pages using the ‘@’ symbol. E.g. @DefenceAustralia
- ❏ Respond in a timely manner to comments and messages if appropriate and necessary.
- ❏ Check notifications to see who is engaging with your content and to monitor engagement.
- ❏ Use hashtags where appropriate
- ❏ Don’t upload more than 5 images at a time

Set up your X account:

1. Sign up for a new account, the “full name” you provide Twitter will be your display name. It can be changed if needed. Use your previously agreed naming convention.
2. Enter a phone number for the person in charge of the account; the phone number is used for two-factor authentication to secure your account. Verify your page when the text from Twitter comes through.
3. Pick a secure password using a variety of upper/lower case, symbols and numbers.
4. Click **settings and privacy** and at the top of this page, you can pick your username. Use your previously agreed handle.
5. Update your profile picture by clicking on **profile** and then **edit profile** on the right under the blue bar. You can upload your profile picture, which should be a high quality 400x400 version of the official emblem relevant to the brand on a white background.
6. Update your cover photo in the edit profile section. Ensure the cover image is high quality approved imagery relevant to the page the size should be 1500 x 500.
7. Update your biography with a short description of the page, this should be previously approved. List defence.gov as the website.

Using your account: How to send a post

1. Type your tweet into the compose box at the top of your home timeline or click the **tweet** button in the top right of the navigation bar. Your tweet cannot exceed 280 characters. It is best to draft your tweet in a scheduling program or an online twitter character counter.
2. You can include four photos, a GIF or a video (no higher than 720p). There are icons at the bottom of the tweet to click to upload any of these items.
3. If scheduling a tweet in another program the process might be slightly different but the limitations on content still apply.

Using your account: How to repost

1. If you come across a post you like you can **repost** this by clicking on the **repost** button.
2. The tweet will pop up giving you the chance to add text to accompany the post you are sharing.
3. If no text is required, click the **repost** button at the bottom of the tweet to instantly share.

Quick tips:

- ❑ Don’t spam your followers
- ❑ Use the @ symbol to reply to others where relevant and necessary
- ❑ If you would like to tag another person or page use the @ symbol.
- ❑ If you start your tweet with an @ symbol put another character such as a full stop in front so that it appears as an original tweet rather than relying to the page. E.g. ‘.@DefenceAust’
- ❑ Use relevant hashtags if the word limit permits.
- ❑ Repost with an over quote if the tweet needs further clarification.
- ❑ Shorten links using a service such as bit.ly

Set up your Instagram account:

1. Download the app and sign up using an appropriate email address, it is best not to sign up using your Facebook account.
2. Create your using name using a previously agreed naming convention.
3. Pick a secure password using a variety of upper/lower case, symbols and numbers.
4. Click done.
5. Your Instagram account is set up.
6. Upload a profile photo by clicking **Edit Profile > Change profile photo** and select an appropriate image. Ensure you use a high quality 110x110 version of the official emblem relevant to the brand on a white background.
7. Update you biography with a short description of the page, this should be previously approved. List defence.gov as the website.

Using your account: How to create a post

1. To upload a photo press the plus symbol at the bottom of the screen on the app.
2. Select the photo you wish to upload. Ensure it is high quality approved imagery or video.

3. Tap on the **write a caption...** section, enter your pre-approved caption. Click **ok** when you are complete.
4. Click **share** to post your image if you are not using a scheduling tool.

Quick tips:

- ❑ Use relevant hashtags.
- ❑ Credit the photographer in the images.
- ❑ Tag relevant pages in the caption.
- ❑ Avoid reposting or sharing images, it is best to have high quality approved content.
- ❑ Do not post too often, once a day or once every few days.

Setting up your LinkedIn showcase page:

Seek assistance for LinkedIn showcase page set-up through the Social Media Hub.

Using your account: How to post to a showcase page

1. Click share an update in the showcase page admin widget on the left of your homepage
2. Below manage, select your page
3. Click the updates tab
4. Enter your update into the share an article, photo, video or idea box at the top of the page
5. Click post to share your update if you are not using a scheduling tool.

Quick tips:

- ❑ Post high quality content relevant to the page
- ❑ Don’t post too often
- ❑ Consider writing longer form posts.

Glossary

General	AI	Artificial intelligence refers to computers or robots controlled by computers able to perform tasks.
	Alerts	Alerts are updates of all relevant mentions online.
	Average Response Time	This is how long it takes to reply to a message or notification.
	Brand Advocate	A person or customer who talks positively about your brand or product.
	Conversion	A positive action taken on a website by which a visitor from social media converts to a customer. For example, newsletter sign up, a downloaded report, or a form filled in, a sale etc.
	Dark Social	The invisible shares that happen through channels like messengers, email, and text messages. For example, the sending of a URL to a friend via email - dark social. They will not know where you found the article. It means that dark social is referral traffic that's hard to track.
	Emoji	Emoji's are ideograms and smileys used in electronic messages and web pages.
	Engagement	Users interacting with a brand by liking, commenting, sharing posts, images, etc.
	Google Analytics	A free service from Google to monitor website traffic.
	ICYMI	In Case You Missed It

Image Recognition	Technology that recognises logos, objects, and scenery so brands can find actionable consumer insights, anticipate a crisis, and measure brand awareness.
Influencer	A social media user who has the potential to reach a relevant audience - large or small - and create awareness about a trend, topic, brand, or product.
Newsjacking	The practice of benefiting from the huge popularity of a current news story to amplify your sales and marketing success.
PPC	Pay per click ads are used to show ads on various websites or search engines, and pay when a user clicks through.
Reach	Post reach - how many unique users who saw your post Page reach - how many users saw any content you posted Organic reach - how many users saw your content, of their own accord Paid reach - how many users saw your promoted piece
Search Engine Marketing (SEM)	An online strategy with the intention of attracting customers, generating brand awareness, and building trust and loyalty. SEM will increase your website's visibility primarily through pay per click ads (PPC).
Sentiment Analysis	An analysis of subjective information from content to understand the attitude of a person/users.
Search Engine Optimisation (SEO)	Search engine optimisation is how to improve the volume or quality of unpaid traffic to a website from search engines. This increases the chances of a website appearing near the top of search engine results pages (SERPs).

Share	Users share message, products, brand awareness, thoughts, and company voice with others users.
Share of Voice | SOV	Percentage of social media posts in a given category. Brands use SOV to find out how their popularity ranks against their competitors.
Snapchat	A social app allowing users to send and receive time-sensitive photos. The images are hidden once the time limit ends.
Social media analytics	Analysis of online conversations to determine brand awareness, online reputation, and measure outcomes of social media strategy, marketing strategies etc.
Social Media Listening (SML)	Finding and tracking online conversations, around keywords, phrases, events, about your brand, business, services and competitors.
Social Media Monitoring (SMM)	Listening and looking at social media channels and responding to mentions related to your business.
Social Media Optimisation (SMO)	Building publicity through social media channels and online communities to drive traffic from sources other than search engines.
Social Media Return on Investment (ROI)	How much a business invests - time, money, resources - in social media in comparison to results from this investment
Social Networking	Socialising in an online community.
Tag	Tagging is a social media functionality, most often used on Facebook and Instagram, to identify a person or place within content.
Thread	Beginning with an original post, the conversation and comments that follow.

Traffic	Visitors to a website.
Trending Topic	The most talked about topics and hashtags on social media.
Trendjacking	Piggybacking a big social trend to get users to engage with a business.
User-Generated Content (UGC)	Content that is shared by people online.
Viral	When a piece of content achieves noteworthy awareness
Webinar	Online seminar or presentation, hosted by an individual or a company.
YOLO	You Only Live Once
YouTube	The biggest platform for video content.

Facebook	***A social network that allows users to interact with others, connect with friends and family, and share photos, video and information.***	
	Events	Set up to reach audience, sell tickets, and measure performance.
	Ad	Create an ad that’s displayed on Facebook.
	Insights	Analytics hub for tracking user interactions on your Facebook Fan Page. Insights include likes, comments, shares, views, traffic source, age, language and gender of your audience.
	Facebook Live	Live video to engage users/followers.
	Messenger	Instant messaging via Facebook.
	Follower	Similar to a fan relationship or a Twitter follow, it allows followers to see posts without having the relationship approved.
	Group	A place for group chat for people who share a common interest - groups are private or public.
	Like	People click Like to show they like the content.
	News Feed	Content that appears in your news feed is influenced by your friends, groups, subscribed pages, and activity.
	Promoted/Boosted Post	Pay to boost a post and get more eyeballs.
	Reactions	An extension of the Like button for expressing emotions: Like Love Haha Wow Sad Angry

	Suggested Pages	Pages you may be interested in, based on previous page views, check-ins, likes, and friends.
	Tabs	Links a range of sections that make a profile, including Home, About, Posts, Events, Videos, Photos, etc.

X	***A social networking site that enables people to share ideas through short texts popularly known as tweets. X is considered as a micro-blogging service due to the users' ability to post information in the form of texts, images and videos and share with friends across the globe.***	
	Hashtag	Hashtags are used in front of words or short phrases to provide context,
	Mentions	When you're looking to tag someone or a brand in a tweet, include @username and they'll receive a notification. It's used to initiate conversations with other users, or attribute content. *Note that if you start a tweet with @username, only your mutual followers will see the tweet. To make it visible to others, use a period before - .@username.*
	DM	A direct message is so you can talk privately to another X user.
	Feed	A list of posts that constantly updates, when new tweets that fit a specified criteria are tweeted.
	Follower	Someone who follows you on X and sees all your posts in their home feed.
	Handle	Your @username on X
	Home Feed	Updates every time someone you follow posts a tweet.

	Like	People click Like to show they like the content. Used to be a star, now represented by a heart symbol.
	MT	Is short for ‘Modified post’, which is when a user is trying to retweet but the tweet's too long so they modify the original tweet.
	Pinned post	You can pin a post to the top of your profile for more exposure.
	Reply	Is responding to a tweet someone has tagged you in with a @mention. A reply is visible to anyone and everyone - even if they don’t follow you.
	RT	Is short for ‘repost’, letting users know where the original content came from

Instagram	***An online mobile photo-sharing and social networking service that enables its users to take pictures and videos, and share them either publicly or privately on the app as well as through a variety of other social networking platforms, such as Facebook, Twitter, Tumblr and Flickr.***	
	Bio	Area for a short description under profile picture.
	Caption	Captions add context to a post, along with a relevant hashtag.
	Comments	The clue's in the word.
	Feed/Gallery/Album	Collection of images posted to your profile.
	Filters	There are 20 filters, including exposure, color balance, contrast, and different frames, to edit photos.
	Follower	A user who follows your account and sees all your published photos.
	Following Activity Feed	A feed of images that people you're following have liked or commented on. Only shows five minutes of information.
	Geotags	The location attached to an image, which corresponds a longitude and latitude on a map. This means your image can be viewed alongside other photos geotagged for this location.
	Hashtags	# used by Instagram and Twitter, a hashtag allows user to connect with others and find images based on a common word. Using a hashtag means others will find it.
	Like	People click Like to show they like the content.

News Feed	Via the Home button on the app, this feed shows image from those you follow.
Personal Activity Feed	Shows you when a user likes or comments on one of your images, when your username is mentioned, wher your image is posted to the popular page, and when you’re tagged in a photo.
Post	Image uploaded to Instagram, can include a caption, geotag, users’ tags etc.

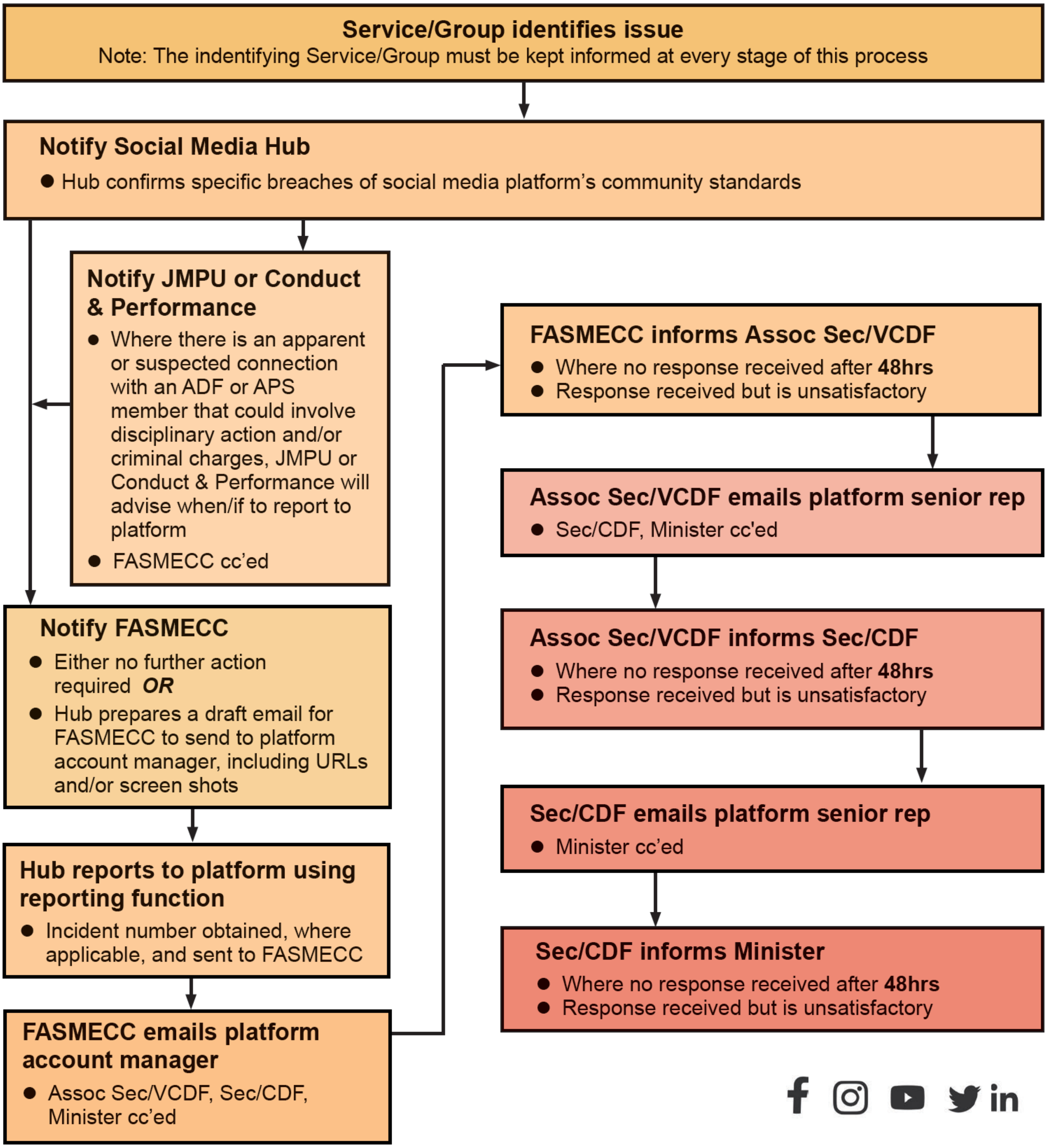
LinkedIn	***A social networking site with individual users and organisations. Individuals can network, build up connections, follow companies, and job hunt. You can share news, blog posts, opinion pieces, and job ads. There are specialized groups to join too.***	
	Company Profile	A biography on LinkedIn that includes connections at the company, new hires, promotions, jobs, related companies, and company statistics.
	Showcase page	A LinkedIn Showcase page is an extension of the Defence Australia page designed to spotlight individual areas and business units and target their own specific audiences.
	Connections	People you invite or people who have invited you on LinkedIn.
	Endorsements	Signposts to other users showing your expertise. It's very quick and easy to endorse, so they don't have the value of a recommendation.
	Groups	Public or private, created by an individual or a company. They allows users to gather and discuss a specific subject.
	Network	Your connections, including the connections of your connections.
	Recommendation	A way to recommend a friend/colleague based on their professional experience, to anyone who views their profile.
	Request	Sent by one user to another, describing a possible project or opportunity.

Australian Government
Department of Defence

REPORTING OF OFFENSIVE CONTENT

Escalation Process

- This flow chart covers the escalation process for **Priority 1** requests for social media platforms to remove offensive content or accounts.
- **Priority 1** matters involve: serious reputational damage, extreme violence, security breaches, threats, sexual misconduct, fear for safety and fraud.



Service/Group identifies issue
Note: The indentifying Service/Group must be kept informed at every stage of this process

Notify Social Media Hub
- Hub confirms specific breaches of social media platform's community standards

Notify JMPU or Conduct & Performance
- Where there is an apparent or suspected connection with an ADF or APS member that could involve disciplinary action and/or criminal charges, JMPU or Conduct & Performance will advise when/if to report to platform
- FASMECC cc'ed

Notify FASMECC
- Either no further action required *OR*
- Hub prepares a draft email for FASMECC to send to platform account manager, including URLs and/or screen shots

Hub reports to platform using reporting function
- Incident number obtained, where applicable, and sent to FASMECC

FASMECC emails platform account manager
- Assoc Sec/VCDF, Sec/CDF, Minister cc'ed

FASMECC informs Assoc Sec/VCDF
- Where no response received after **48hrs**
- Response received but is unsatisfactory

Assoc Sec/VCDF emails platform senior rep
- Sec/CDF, Minister cc'ed

Assoc Sec/VCDF informs Sec/CDF
- Where no response received after **48hrs**
- Response received but is unsatisfactory

Sec/CDF emails platform senior rep
- Minister cc'ed

Sec/CDF informs Minister
- Where no response received after **48hrs**
- Response received but is unsatisfactory

Reporting offensive profiles content

Task: Reporting offensive third party content through respective platforms and liaison officers

Last revised (date): 19/06/2020

SOP Ref.: #

Purpose: Reporting, for the purpose of removing, offensive third party content on unofficial social media pages through both the platform and the respective liaison officers for each platform.

Scope: These standard operating procedures are to be used in conjunction with the relevant Defence social media policies including but not limited to the Media and Communication Policy and the Social Media Playbook.

Prerequisites:

- Sound knowledge of MS Outlook

s47E(d) [redacted]

- Access to administrative Defence social media accounts on all platforms

s47E(d) [redacted]

Responsibility:

- To ensure all identified and reported offensive third party content is reported and removed as quickly as possible from the respective social media platforms.
- To ensure all stakeholders are informed and updated on the progress on content reporting and removal.
- To ensure the media team are aware of any and all ongoing offensive third party content removal processing.

Frequency: As required

Timing: As required

Information and access requirements:

s47E(d) [redacted]

- Access to MS Outlook

s47E(d) [redacted]

- Access to administrative Defence social media accounts on all platforms

s47E(d) [redacted]

STANDARD OPERATING PROCEDURES: DEFENCE SOCIAL MEDIA HUB

PROCESS STEPS

Before taking action, ensure you are logged out of all your social media accounts and have opened a new browser session.

Receiving a notification for offensive third party content

Emails will come to the Defence Social Media Hub inbox from either internal department employees or from members of the public who have identified offensive third party content. Before the process can proceed, ensure that you have the following information:

1) Account URL
2) Account name
3) Image/screenshot of offensive content
4) Date of content posting
5) Reporting party email

Where the information above hasn't been provided, contact the individual who has sent the email and request further information. Some of the information above can be deduced from the image/screenshot provided.

Identifying the process action

Review the main social media channels (Facebook, Twitter, Instagram, LinkedIn, YouTube) for third party memes profiles posting inappropriate content relevant to, or directed at, the Department of Defence and the Australian Defence Force (ADF).

These profiles can be found by:

s47E(d)

Using the platforms search functions and using common terms like "ADF, diggers, memes, lid, etc."

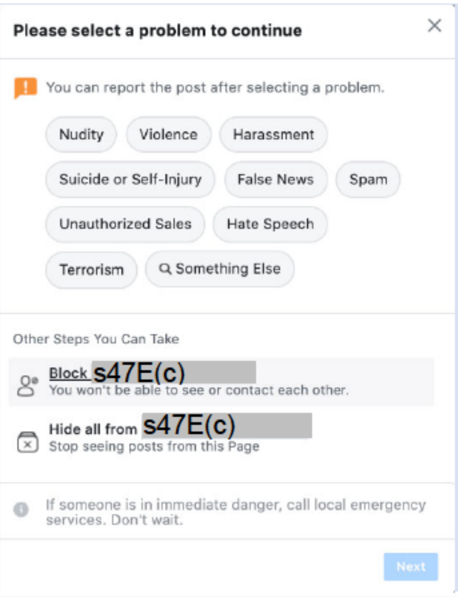
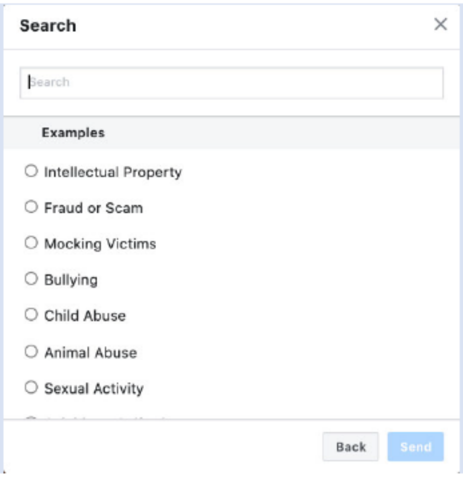
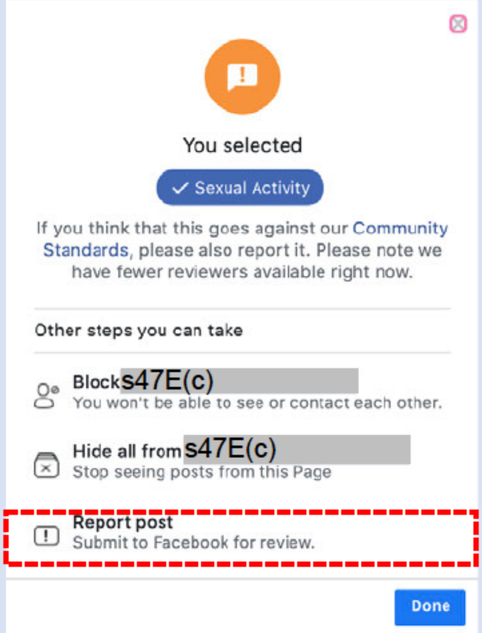
Content can be reported and removed for one of the following categories:

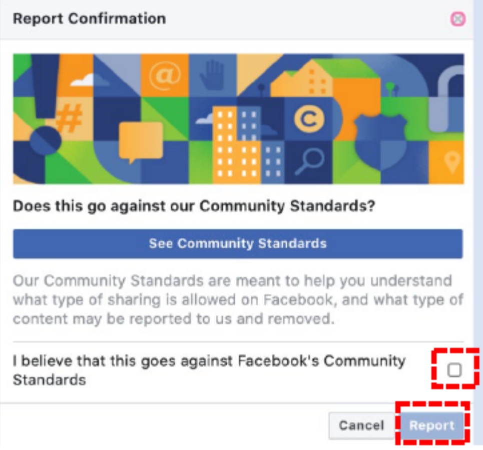
Nudity	**Violence**	**Harassment**	**Suicide or self-injury**	**False news**
Unauthorised sales	**Hate speech**	**Terrorism**	**Promoting drug use**	**Spam**
Non-consensual intimate images	**Sexual exploitation**	**Sharing private images**	**Intellectual property**	**Fraud of scam**
Bullying	**Child abuse**	**Animal abuse**	**Sexual activity**	**Mocking victims**

Follow the steps below to report the image through each platform.

Facebook reporting

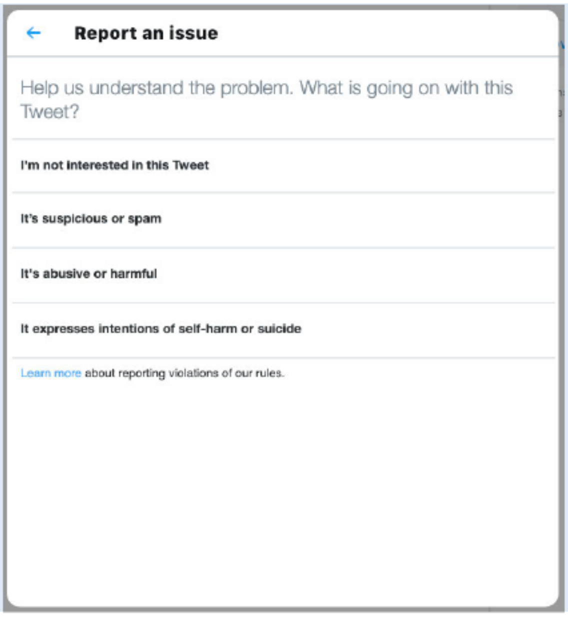
Facebook – report a post		
Step	Image	Instructions
1	s47E(c) [redacted]	Find the post with offensive content.
2	[redacted]	Select the options "..." button at the top right of the post. Then select the "Find support or report post" option at the bottom of the list.

3	 Please select a problem to continue You can report the post after selecting a problem. Nudity Violence Harassment Suicide or Self-Injury False News Spam Unauthorized Sales Hate Speech Terrorism Something Else Other Steps You Can Take Block s47E(c) You won't be able to see or contact each other. Hide all from s47E(c) Stop seeing posts from this Page If someone is in immediate danger, call local emergency services. Don't wait. 	A box will appear containing reporting categories. If the category you find most suitable isn't available, select the "Something Else" option and next and see step 4. Otherwise, select the option and move to step 5.
4	 Search Examples ○ Intellectual Property ○ Fraud or Scam ○ Mocking Victims ○ Bullying ○ Child Abuse ○ Animal Abuse ○ Sexual Activity 	The "something Else" button will provide a list with all alternate reporting categories. Select the option you think is suitable then hit next.
5	 You selected ✓ Sexual Activity If you think that this goes against our Community Standards, please also report it. Please note we have fewer reviewers available right now. Other steps you can take Block s47E(c) You won't be able to see or contact each other. Hide all from s47E(c) Stop seeing posts from this Page Report post Submit to Facebook for review. 	Select the "Report post" button.

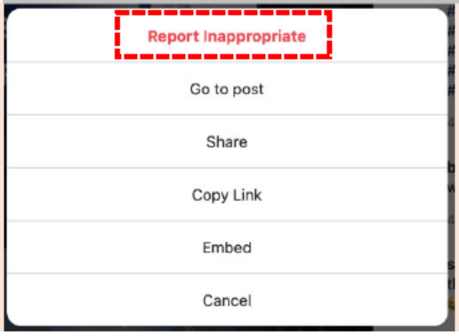
6	 Report Confirmation Does this go against our Community Standards? See Community Standards Our Community Standards are meant to help you understand what type of sharing is allowed on Facebook, and what type of content may be reported to us and removed. I believe that this goes against Facebook's Community Standards □ Cancel Report	Tick the box and select report. Should you need to create an email to a liaison officer, you can find the Facebook Standards through the "See Community Standards" button. s47E(d)

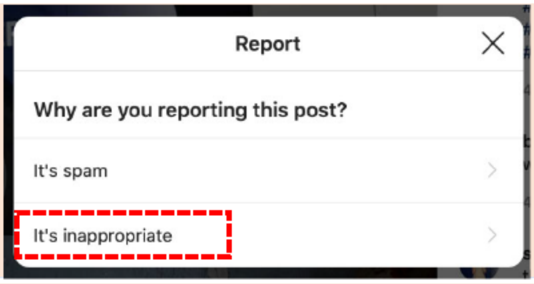
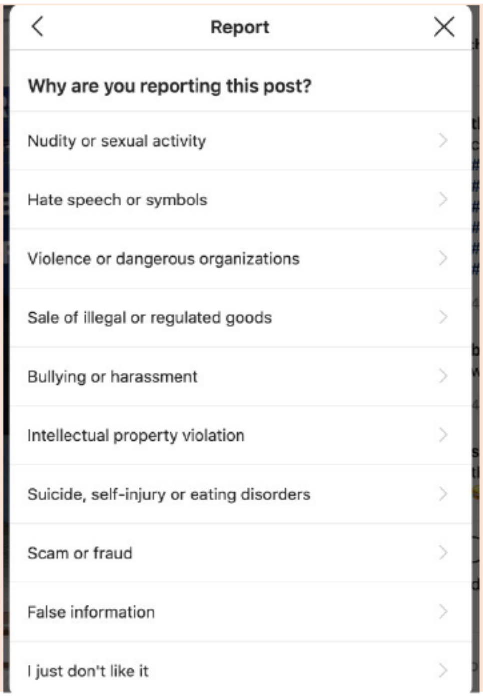
Twitter reporting

Twitter – report a post		
Step	**Image**	**Instructions**
1	s47E(c)	Find the post with offensive content. Select the options "v" button at the top right of the post.
2		Then select the "Find report tweet" option at the bottom of the list.

3	 Report an issue Help us understand the problem. What is going on with this Tweet? I'm not interested in this Tweet It's suspicious or spam It's abusive or harmful It expresses intentions of self-harm or suicide Learn more about reporting violations of our rules.	Select the option that best suits the inappropriateness of the content. s47E(d) s47E(d)

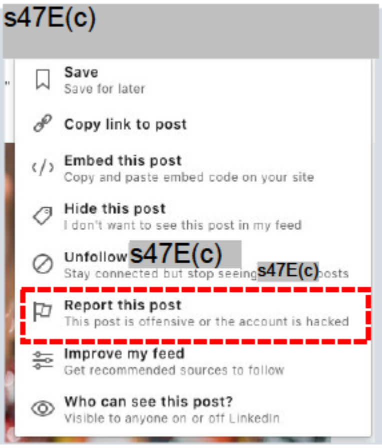
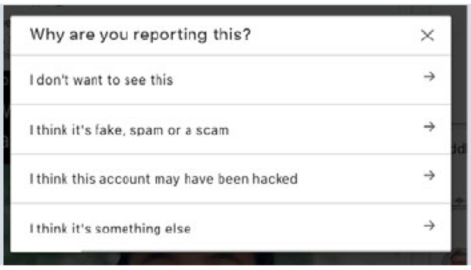
Instagram reporting

Twitter – report a post		
Step	Image	Instructions
1	s47E(c)	Find the post with offensive content. Select the options "…" button at the top right of the post.
2	 Report Inappropriate Go to post Share Copy Link Embed Cancel	Then select the "Report Inappropriate" option at the top of the list.

3	 Report Why are you reporting this post? It's spam It's inappropriate	Then select the "It's inappropriate" option at the bottom of the list.
4	 Report Why are you reporting this post? Nudity or sexual activity Hate speech or symbols Violence or dangerous organizations Sale of illegal or regulated goods Bullying or harassment Intellectual property violation Suicide, self-injury or eating disorders Scam or fraud False information I just don't like it	Select the option that best suits the inappropriateness of the content. s47E(d) [redacted] s47E(d) [redacted]

LinkedIn reporting

LinkedIn – report a post		
Step	**Image**	**Instructions**
1	s47E(c) [redacted]	Find the post with offensive content. Select the options "…" button at the top right of the post.

2	 s47E(c) Save Save for later Copy link to post Embed this post Copy and paste embed code on your site Hide this post I don't want to see this post in my feed Unfollow s47E(c) Stay connected but stop seeing s47E(c) posts Report this post This post is offensive or the account is hacked Improve my feed Get recommended sources to follow Who can see this post? Visible to anyone on or off LinkedIn	Then select the "Report this post" option in the list.
3	 Why are you reporting this? I don't want to see this I think it's fake, spam or a scam I think this account may have been hacked I think it's something else	Select the option that best suits the inappropriateness of the content. s47E(d) s47E(d)

You have now successfully reported the post through the platform. You will receive a response through the platform to the success of your report. It will explain whether the platform agrees and has removed the post, or if it does not think it violates the standards.

s47E(d)

s47E(d)

[redacted]

s47E(d)

Progressing content reporting through liaison officer

Where a negative response is received from the platform, you can take the reporting to the next step by emailing the liaison officer for double verification.

Facebook

Complete this web form https://www.facebook.com/business/help.

1. Select the 'Something Else' option.

2. Use this script in the 'Please let us know how we can help *' field

> Hello,
>
> A Facebook [profile/page/group] called [insert name], [insert link], is [detail offences].
>
> The Department of Defence's Social Media team would like to request that the [profile/page] be deleted for the following breaches of Facebook Community Standards:
>
> [List the applicable Facebook Community Standards].
>
> We have already reported the page on Facebook.
>
> Please remove this [profile/page/group] asap. Please advise.
>
> Kind regards,
> [insert name].

** Attach screenshots of the [profiles/pages/groups] and their posts.*

Twitter

s47F @twitter.com. Use this script:

> **Subject:** Reporting Twitter profiles
>
> **Body:** Hi s47F
>
> Hello,
>
> A Twitter profile called [insert name], [insert link], is [detail offences].

The Department of Defence's Social Media team would like to request that the profile be deleted.

We have already reported the profile on Twitter.

Please remove this profile asap. Please advise.

Kind regards,
[insert name].

** Attach screenshots of the profiles and their posts.*

LinkedIn

Email linkedin_support@cs.linkedin.com. Use this script:

Subject: Reporting LinkedIn [profiles/company pages/showcase pages/groups]

Body: Hello,

A LinkedIn [profile/company page/showcase page/group]. called [insert name], [insert link], is [detail offences].

The Department of Defence's Social Media team would like to request that the [profile/company page/showcase page/group] be deleted.

We have already reported the [profile/company page/showcase page/group] on LinkedIn.

Please remove this profile asap. Please advise.

Kind regards,
[insert name].

** Attach screenshots of the [profiles/pages/groups] and their posts.*

Instagram

**same process as Facebook as owned by same company*

Complete this web form https://www.facebook.com/business/help.

1. Select the ‘Something Else’ option.

2. Use this script in the ‘Please let us know how we can help *’ field

Hello,

A Facebook [profile/page/group] called [insert name], [insert link], is [detail offences].

The Department of Defence's Social Media team would like to request that the [profile/page] be deleted for the following breaches of Facebook Community Standards:

[List the applicable Facebook Community Standards].

We have already reported the page on Facebook.

Please remove this [profile/page/group] asap. Please advise.

Kind regards,
[insert name].

** Attach screenshots of the [profiles/pages/groups] and their posts.*

YouTube

Email s47F @google.com. Use this script:

Subject: Reporting impersonation YouTube [accounts/channels]

Body: Hi s47F

A YouTube [account/channel]. called [insert name], [insert link], is [detail offences].

The Department of Defence's Social Media team would like to request that the [account/channel] be deleted.

We have already reported the account on LinkedIn.

Please remove this account asap. Please advise.

Kind regards,
[insert name].

** Attach screenshots of the [accounts/channels] and their posts.*

Verifying a notification for offensive third party content

When the Social Media Hub are notified of offensive content, it is process to reply to the reporting individual with the intent to remove. In order to establish he likely next steps, the content must be investigated. Access the content using the URL provided (or find the page using the account name).

Responding to a member of the public who has identified offensive third party content

When responding to a member of the public regarding identified offensive third party content, use the email script below.

Subject: RE: Identified offensive third party content

Body: Good morning/afternoon,

Thank you for your email.

The Department of Defence's Social Media team will investigate this matter and progress as appropriate.

Kind regards,
[signature].

b. **Official positional:** approved accounts are operated by Defence personnel for a Defence purpose related to a position (e.g. Chief of the Defence Force Facebook account, Chief of Air Force Twitter account etc.). Official positional accounts must be handed over when the person completes their tenure.

DEFENCE SOCIAL MEDIA HUB

6.5 The Defence Social Media Hub is responsible for:

a. whole-of-Defence social media strategy, policy, process, training, content guidance, crisis management, analytical reporting, technical support, and account consolidation;

b. gaining approval and providing access to social media software and tools;

c. reporting on the number and usage of official social media accounts;

d. maintaining the whole-of-Defence Social Media Playbook, which provides guidance on social media best practice;

e. coordinating the Defence Social Media Working Group; and

f. being the point of contact for Groups and Services to report suspected offensive content on social media by or about Defence personnel and to escalate in accordance with the Reporting of Offensive Content Escalation Process.

6.6 Authorised practitioners are to provide performance information, metrics and analytics of all official Defence social media accounts to the Defence Social Media Hub in support of an annual review.

6.7 For further information, including instructions on the correct use and best practice of official social media accounts, refer to the Social Media Playbook on the Defence Social Media intranet page, or contact the Defence Social Media Hub.

PRINCIPLES OF OFFICIAL DEFENCE SOCIAL MEDIA ACCOUNTS

6.8 There are three principles for all official Defence social media accounts:

a. Accountability at a senior level within the chain-of-command.

b. Alignment with government policy and Defence objectives.

c. Priority for high-profile announcements, key decisions, operations, events and other significant content lies with the Government to ensure that:

i. social media accounts do not pre-empt or foreshadow government decisions or operational, capability or policy outcomes unless authorised by the Assistant Secretary Media and Information Disclosure (ASMID);