# Social Media Procedure

## Contents

## Context

1. This procedural document is to be followed in accordance with the ACC Social Media Policy.

2. All members of the staff of the ACC[1] are directed to and **must** comply with the 'must' or 'must not' controls as well as any legislative controls outlined within this Policy. Failure to do so may result in Code of Conduct action and any breach of the obligation on members of staff under section 51 of the *Australian Crime Commission Act 2002* (the ACC's secrecy provision), may result in criminal prosecution. Unauthorised disclosure of information may be punishable by 2 years imprisonment and/or fine not exceeding 120 penalty units.

3. Should definitions be required they are contained within the Policy.

## Determining When or How the Policy Applies

4. This policy and procedure addresses any **personal** use of social media. Online social media can take many forms, including (but not limited to) social networking services, chat rooms, weblogs, social blogs, wikis, podcasts, internet forums, dating sites, etc. It can be any site that allows users to post dialogue, pictures and/or video, and includes technologies such as picture-sharing, email, instant messaging; and websites such as YouTube.

5. This policy and procedure does not apply to business use of social media.

## Responsibilities for Staff

6. When using online social media and/or social networking services in a private capacity, staff **should not** identify themselves as an ACC staff member. SES staff, and executive level staff with written SES approval, may identify themselves as an ACC staff member on professional networking sites such as LinkedIn only after proactively considering the risks identified in this policy and procedure. When using online social media and/or social networking services in a private capacity staff **must not** identify, or enable someone to reasonably identify, another ACC staff member.

7. Staff **must not** make any comments or postings concerning ACC business. When considering whether to make comment in an unofficial capacity, staff should also reflect on the following questions:

    - Could the comments reasonably be expected to cause the ACC's clients and other stakeholders, including members of parliament – whether members of the Government, the Opposition, independents, or other parties – to lose confidence in the staff members ability to work in an impartial and professional manner?



[1] All members of the staff of the ACC as defined in the ACC Act and may be referred to herein as staff.

- Would comment of this kind, without proper justification, be likely to lower or undermine the reputation of the ACC or of the APS as a whole?
- Are these comments in line with how the community in general expects the public service to operate and behave?
- Are these comments lawful? For example, do they comply with anti-discrimination legislation and laws relating to defamation?

8. When posting in a private capacity, do not make any comment or posting which may be interpreted as representing the views of the ACC or contain any material that may potentially bring the ACC or the APS in general into disrepute.
9. Even in a private capacity, inappropriate public comment by staff may result in sanctions as a result of a breach of the APS Code of Conduct.

## Risks in Using Online Social Media and Networking Sites

10. There are risks associated with participating in online social media and networking sites online. The speed and reach of online communication means that it can never be certain where the comment might end up or who might read it. Material posted online effectively lasts forever. It may be replicated endlessly, and may be sent to recipients who were never expected to see the post or may view it out of context.
11. Any information relating to employment that is posted online (including naming a staff member or describing a professional role or responsibility) is able to be located quickly and easily by a search engine. Posting career information online can inadvertently disclose corporate information and poses a potential security risk.
12. Corruption of public officials can provide benefits for organised crime groups and public sector officials may be targeted for this reason. Information posted on social media sites may be used by criminals to gather information on staff and their family, friends and associates in an attempt to identify those who may be susceptible to corruption and groomed for this purpose. Data mining (using data to predict trends or behaviour patterns) is also used by cyber thieves to obtain information for criminal purposes.
13. Staff **must** comply with this policy and procedures even when they are posting material anonymously, or using an alias or pseudonym. Even if you do not identify online as an ACC employee you could still be recognised as such.
14. Remember that inappropriate use of social media sites can compromise you, your family, friends and colleagues as well as jeopardise your career.

## Inappropriate or Unacceptable Use of Social Media

15. The following (non-exhaustive) list provides some examples of social media use that is considered inappropriate or unacceptable:
    a. unauthorised discussion or disclosure of any agency-related information (e.g. ACC projects, policy development, corporate information and day-to-day work). This

could be considered misuse of official information and may result in criminal proceedings as well as action under the APS Code of Conduct;

b. unauthorised discussion of any operational or legal matters in which the ACC is materially involved (e.g. joint operations or matters before the courts);

c. unauthorised comment or information dealing with the infrastructure, hardware, software, security etc. of ACC IT systems;

d. making personal comments or expressing opinions that could be misconstrued as official comments (e.g. expressing opinion on proposed or current policy both as it relates to the ACC and the government of the day);

e. personal attacks on ACC staff, clients or individuals from other APS agencies. This includes belittling or making fun of a colleague or client, or engaging in any type of behaviour that could be considered bullying or harassment either directly or indirectly;

f. posting unauthorised photos or video-clips of ACC activities. This includes identifying current work locations;

g. posting any material subject to copyright (e.g. logos, crests, insignia, etc.) without express permission;

h. posting of any ACC email address, telephone number or other contact details.

## Privacy Considerations

16. There are privacy risks associated with using online social media and/or social networking services. Such sites have varying levels of security and all are vulnerable to security breaches. Before posting personal information, remember that giving out information about yourself online makes it easier for people who are online, and do not know you personally, to find you offline. Think carefully about who you want knowing information such as where you live, your date of birth, your phone number, where you work, what type of work you do and what interests you have.



## Version Control

| Implementation Date | Version | Business Owner | TRIM Link | Revision Number |
|---|---|---|---|---|
| June 2015 | 1 | NM IP&F | trim:[15/93248] | Revision 7 |
| July 2015 | 2 | NM IP&F | trim:[15/93248] | Revision 8 |
| Month Year | # | Position | TRIM Link | Revision Number |