Social Media Policy

Policy No:	DSSCorp-031
Purpose:	The Department of Social Services (DSS) Social Media Policy outlines protocols for using social media to undertake official departmental business, and provides guidance for employees in their personal use of social media.
Category:	**Corporate**
Applicable to:	This policy applies to all DSS employees across all offices.
Relevant Authority:	APSC Circular 2012/1: Revisions to the commission's guidance on making public comment and participating online (social media)
Related Documents:	APS Code of Conduct APS Values Social Media Terms of Use ICT Code of Conduct Bullying and Harassment Policy Recordkeeping Policy Risk Management Framework Web Accessibility
Policy Statement:	DSS is committed to ensuring employees are aware of, and understand the Social Media Policy; enabling them to participate professionally or personally, while being mindful of their responsibilities as DSS and Australian Public Service (APS) employees.
Approved by:	People and Communications Sub-committee
Review Date:	1 December 2015
Policy Owner:	Communication and Media Branch
First Issued	1 December 2014
Document Change Control	This document updates the former DSS social media guidelines for employees.

Table of Contents

1   Introduction

The Social Media Policy outlines protocols for using social media to undertake official DSS business, and provides guidance for employees in their personal use of social media.

The policy aims to inform DSS employees how to use social media effectively and appropriately, within DSS and APS guidelines. It has been developed to assist employees to use social media, so they feel empowered to participate, while being mindful of their responsibilities.

The Social Media Policy applies to all DSS employees, including employees on secondment to DSS, employees on leave, non-ongoing employees and contractors. Managers should ensure their employees are aware of and understand this policy.

This policy should be read in conjunction with the Social Media Terms of Use, which set out the rights and expectations of DSS when engaging with the public through DSS social media accounts.

2   Policy

The Social Media Policy applies to the official use of social media, where employees have been authorised by the Department's Communication and Media Branch (CMB) to use social media as a communication tool, to engage with the community, or to distribute content on behalf of DSS. This includes posting to an official departmental social media account (e.g. DSS Twitter), participating as a departmental representative on a third-party site (e.g. external blog, news comment, online forum) or utilising internal online engagement tools and platforms (e.g. STAFFnet blogs).

This policy also provides guidance to employees in their personal use of social media. Employees are reminded of their responsibilities under the APS Code of Conduct and APS Values, which apply when using social media, either professionally or personally.

3   Official use of social media

The same high standards of conduct and behaviour generally expected of public servants also apply when participating online through social media. Online participation should reflect and uphold the values, integrity and reputation of DSS and the APS.

CMB manages and authorises the use of all official DSS social media accounts. Communication Account Managers are responsible for engaging online with stakeholders and the general public in an official capacity. In some cases, authorised employees from other business areas may be asked to assist CMB with this work, and they will be trained accordingly.

Comments made from DSS social media accounts must not:

- endorse or make judgements about specific providers, products or services
- discuss circumstances surrounding DSS' specific relationship with or management of service partners or providers
- make personal judgements about how providers have implemented programme guidelines
- represent or speak on behalf of another DSS business area (i.e. don't discuss other business without the prior consent and advice of the relevant business area).

If an online discussion involves specific individual circumstances or personal details, the moderator must 'switch channel' by directing members of the public to an alternative medium (e.g. telephone, direct message, email, letter, face-to-face) as appropriate.

3.1 Key principles for official use of social media

All employees who are authorised to use or deploy social media as an official communication tool need to be familiar with, and apply the following key principles:

Approved activity – before commencing a social media initiative, your activity must be supported by a business case, and approved by CMB.

Risk management – to ensure risk controls are effectively implemented and monitored, a Risk Management Plan must accompany the business case for a social media initiative.

Administration – an official DSS social media account must be administered by an authorised Communication Account Manager in CMB.

Identity and authenticity – always use an authorised departmental identity (usually the official DSS social media account/handle) and not a personal identity when posting to, or responding from DSS social media accounts, on behalf of DSS.

Maintain confidentiality – only post publicly available information. Don't disclose or discuss official or classified information, make commitments or engage in activities on behalf of DSS or the Government, unless you are authorised by the appropriate business area to do so.

Protect and respect privacy – check the account privacy settings are appropriate for the scope of engagement you wish to undertake. Protect your own privacy and personal information. Don't share the private details of others. Don't disclose details of private conversations unless you have obtained explicit consent from the relevant parties.

Be impartial – avoid statements that advocate or criticise policies of government or political parties. Avoid conflicts of interest through endorsement or criticism of third-party providers, partners, products or services. Avoid expressions of personal opinion.

Be respectful – be courteous and polite. Be sensitive to diversity. Avoid arguments and don't make personal attacks. Do not post obscene, defamatory, threatening, harassing, discriminatory or hateful content.

Be accurate – make sure the information you publish is correct and cite sources where appropriate – people may make decisions based on information you post. Only post on your area of expertise and refer to an appropriate business area where necessary.

Consider intellectual property – respect copyright. Always get permission to use words, images or materials online that you do not own. Any use of DSS departmental branding and logos must be approved by CMB.

Make a record - keep records of social media posts you make in an official capacity. Classify and store information as set out in the Recordkeeping Procedures.

Think first – review your content before you post it. Remember that you are responsible for your actions. You should consider the impact your activities could have on yourself and/or DSS. Use your common sense and best judgement. If you're not sure, check with your manager first.

If in doubt, leave it out!

4 Personal use of social media

DSS employees should be aware that content published on social media is, or may become publicly available, even from personal social media accounts. Employees must ensure they:

- are mindful that their behaviour is bound by the APS Values and Code of Conduct and the DSS ICT Code of Conduct – even outside work hours and when material is posted anonymously or using an alias or pseudonym
- make clear that any views expressed are their own, and not those of DSS
- don't use a work email address to register personal social media accounts
- don't make comments that are obscene, defamatory, threatening, harassing, discriminatory or hateful to, or about work, colleagues, peers or the APS
- don't post comments or images that are, or could be perceived to be:
    - made on behalf of DSS or the Government
    - so harsh or extreme in criticism that they raise questions about the capacity to work professionally or impartially as an APS employee (such comments would not have to relate directly to their area of work)
    - compromising the capacity to fulfil duties as an APS employee in an impartial and unbiased manner. This applies particularly where comment is made about DSS policies and programmes
    - so strong in criticism of DSS' administration that it could seriously disrupt the workplace. (Employees are encouraged to resolve concerns in discussion with a manager or via internal dispute resolution mechanisms)
    - unreasonable criticism of DSS clients or other stakeholders
    - compromising public confidence in DSS or the APS.

When considering making personal comments, employees should reflect on the following questions:

- could my comments cause DSS' clients or other stakeholders to lose confidence in my ability to work in an impartial and professional manner?
- are my comments consistent with how the community expects the public service to operate and behave?
- could my comments lower or undermine the reputation of DSS or the APS?
- are my comments lawful? For example, do they comply with anti-discrimination legislation and laws relating to defamation?
- would I be comfortable if my manager read my comments?

4.1 The Internet is forever

What you publish on the internet can remain public for a long time. Content can also be replicated and shared beyond the original intended audience and sent to recipients who were never expected to see it, or who may view it out of context. You should be aware that according to the terms and conditions of some third-party sites, the content you create is the property of the site where it is posted and so may be re-used in ways which you had not intended.

Before you post to a social media site you should understand the tool/platform you are using. It is recommended that you read the terms of service and user guides and look through existing content to get an idea of the posting etiquette and any cultural and behavioural norms associated with the social media platform you intend to engage with.

You should not rely on a social media site's security settings as a guarantee of privacy. You should also adjust your privacy settings according to your own needs. Bear in mind, even if you do not identify yourself online as a DSS or APS employee, you could nonetheless be recognised as such.

5   Responsibilities

5.1   Access to social media at work

Access to social media sites (e.g. Facebook and Twitter) on DSS ICT resources is provided to employees so long as they abide by the DSS ICT Code of Conduct. Personal use is accepted by DSS , however use of DSS ICT resources for private purposes must be undertaken within the constraints outlined in the ICT Code of Conduct.

5.2   Bullying and harassment

DSS is committed to achieving a workplace free of bullying and harassment. For more information, refer to the Bullying and Harassment Policy.

The Australian Public Service Commission (APSC) has also prepared guidance on cyber bullying and online harassment of APS employees by clients or members of the public, which may be experienced through the increased use of social media and other online networking tools. The guidance ensures a consistent approach across all APS agencies to managing instances of cyber bullying and to support employees who may become targets of online abuse in the course of their work.

5.3   Accessibility

DSS is committed to social inclusion and provides support for people with disabilities. In 2011, Media Access Australia undertook research to determine how the accessibility issues found in each of the most popular social media tools can be overcome. Users with disabilities contributed advice on how to overcome inaccessible features. Full report: Sociability: social media for people with a disability.

Where possible, content on official DSS social media accounts should also be made available in an alternative accessible format. This alternative may be represented on DSS internet sites, however given the online interaction inherent in social media, it may also be appropriate to refer individuals to telephone or face-to-face channels.

5.4   Recordkeeping

Information that provides evidence of business activity or decision is a public record. All DSS employees have an obligation to ensure that key decisions and events are recorded in a way that captures the important features of a discussion or decision, presents a faithful and accurate account and can be easily retrieved when needed.

Social media platforms are often provided by third-party providers and are not official recordkeeping systems. By managing content in DSS social media accounts, you accept responsibility for recordkeeping in accordance with the Recordkeeping Policy, ensuring appropriate records are created and captured for all the business functions, activities and transactions.

DSS employees are required to appropriately classify and store information as set out in the DSS Recordkeeping Procedures.

5.5 Privacy

Personal details cannot be provided to third-parties without the explicit consent of the owner. The email addresses of your colleagues and other identifiable information must be treated with discretion and care. DSS employees are reminded not to upload contacts from departmental (Outlook) contacts when using, or prompted by external social networking sites.

6   Sanctions for non-compliance

As a member of the Australian Public Service your behaviour, both in and out of the workplace, must be consistent with the APS Values, the APS Code of Conduct and the DSS ICT Code of Conduct.

A failure to comply with this Policy may constitute a breach of the APS Code of Conduct. Examples of failure to adhere to the Code of Conduct in a social media setting include:

- making derogatory or obscene posts about a manager on a social networking site
- posting derogatory comments or images about welfare recipients from a personal account
- disclosing non-publicly available information about income payments in a blog post.

A suspected breach of the Code - when referred to the Workplace Relations and Conduct Section, People Branch - may be investigated under the Secretary's Procedures for Determining Breaches of the Code of Conduct and for Determining Sanction (the Secretary's Procedures) to determine whether an employee has breached the Code and for determining sanction. These procedures are established under subsection 15(3) of the *Public Service Act 1999* (the Act). If an employee is found to have breached the APS Code of Conduct, the Secretary (or delegate) may determine that it is appropriate to impose sanctions. Section 15(1) of the Act provides for the following sanctions:

- termination of employment
- reduction in classification
- reassignment of duties
- reduction in salary
- deductions from salary, by way of fine
- reprimand.

7   Frequently Asked Questions

7.1   What is Social Media?

Social Media are online services and tools used for publishing, sharing and discussing information. These can include:

- social networking – e.g. Facebook and MySpace
- video and photo sharing – e.g. Flickr, YouTube
- blogs – e.g. corporate blogs, personal blogs or media blogs
- micro blogs – e.g. Twitter
- forums and discussion boards – e.g. Reddit, Whirlpool, Yahoo! Groups
- online encyclopaedias – e.g. Wikipedia, wiki.

7.2   Why use social media?

"Agencies should support employee-initiated, innovative Government 2.0-based proposals that create, or support, greater engagement and participation with their customers, citizens and/or communities of interest in different aspects of the agency's work. They should create a culture that gives their staff an opportunity to experiment and develop new opportunities for engagement from their own initiative, rewarding those especially who create new engagement/participation tools or methods that can quickly be absorbed into the mainstream practice that lifts the performance of the department or agency." Source: Getting on with Government 2.0 | Government 2.0 Taskforce, 2010).

7.3   What is Open Government?

DSS is committed to the principles of *Open Government*:

- **transparency** in process and information
- **participation** by citizens in the governing process
- **public collaboration** in finding solutions to problems and improving the well-being of the community.

Making public comment online is increasingly common for APS employees in a range of capacities, including official, professional and private use. DSS recognises the value in using social media to build more interactive relationships with customers, communities and other relevant stakeholders.

Accordingly, DSS is committed to engaging effectively with citizens in a meaningful, accountable, responsive and equitable way. When used appropriately, social media allows DSS employees to represent DSS and its diversity to the community at large.

7.4   How can social media help me to do my work?

Social media can help with:

- engaging with stakeholders using familiar and widespread technology
- developing a more active relationship with stakeholders and target audiences
- gaining a better understanding of attitudes towards DSS programmes and initiatives
- increasing the speed and frequency of public engagement
- increasing trust through greater transparency
- improving the delivery of services, particularly to rural and remote communities
- facilitating innovation through collaboration with third-parties and industry experts
- organisational and individual development through the open exchange of information, perspectives and opinion
- promoting and marketing DSS activities, both within DSS and to the broader community.

8   More information

If you require assistance in interpreting any part of this policy, or would like to investigate the use of social media for your business area, please contact your Communication Account Manager or email socialmedia@dss.gov.au.