Australian Government
Australian Customs and Border Protection Service

INSTRUCTIONS AND GUIDELINES

Responsible Use of Online Social Media and Online Social Networking Services

January 2012

This Instruction & Guideline refers to Practice Statement:
PS 2010/04 Procedures for determining breaches of the Code of Conduct

Published date:	18 January 2012
Availability:	Internal only
Subject:	Responsible use of online social media and online social networking services
Purpose:	To inform Customs and Border Protection employees of their obligations and responsibilities under the APS Values and Code of Conduct when using online social media and/or online social networking services.
Owner:	National Director, People and Place
Category:	People
Contact:	Director Employee Conditions, People & Place Strategy & Policy Branch (Contact 02 6274 4971)

The electronic version published on the intranet is the current Instruction and Guideline.

BCS CLASSIFICATION: Pers_Policy_Social Networking

FILE NUMBER: 2010/055266

Summary of main points

- The purpose of this Instruction and Guideline is to inform Customs and Border Protection employees who use online social media and/or online social networking services of their responsibilities under the APS Values and Code of Conduct.

This I&G applies to staff in:

- All work areas of Customs and Border Protection, including ongoing and non-ongoing, Customs Flexible Employees (CFEs) and Senior Executives.

Introduction

It is essential that Customs and Border Protection employees fully understand the APS Values and Code of Conduct, and how these apply to both official and personal communications.

Online social media and online social networking services are widely used by people to communicate and socialise with friends and people with similar interests. Employees who participate in these types of activities, whether in the course of their APS employment or privately, must exercise care to ensure their behaviour does not conflict with their responsibilities as employees of Customs and Border Protection or the Australian Public Service in general.

This Instruction and Guideline outlines:

1. A definition of online social media and online social network services;
2. Employee obligations and responsibilities under the APS Values and Code of Conduct when using online social media and/or online social networking services in the course of employment;
3. Employee obligations and responsibilities under the APS Values and Code of Conduct when using online social media and/or online social networking services for personal use;
4. Examples of use that may be considered inappropriate or unacceptable;
5. The potential consequences of inappropriate or unacceptable use; and
6. Privacy considerations.

Instructions and Guidelines

1. Definitions

Online social media can take many different forms, including (but not limited to) online social networking services, chat rooms, weblogs, social blogs, wikis, podcasts, internet forums, dating sites, etc. It can be any website 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.

An online social networking service can be any website or platform that builds online communities of people who share interests and/or activities; and/or enables users to create and/or maintain social relations over the internet. *Facebook, MySpace, Linked In, RSVP* and *Twitter* are some examples of online social networks, but there are many others.

2. Employee obligations and responsibilities under the APS Values and Code of Conduct when using online social media and/or online social networking services in the course of employment

The Australian Public Service Circular 2009/6: *"Protocols for online media participation"*, reminds all APS employees that the APS Values and Code of Conduct, and Public Service Regulation 2.1, also apply when working with online media in the course of their employment. When working with online media, all employees must ensure they are:

- being apolitical, impartial and professional;
- behaving with respect and courtesy, and without harassment;
- dealing appropriately with information, recognising that some information needs to remain confidential;
- delivering services fairly, effectively, impartially and courteously to the Australian public;
- being sensitive to the diversity of the Australian public;
- taking reasonable steps to avoid conflicts of interest;
- making proper use of Commonwealth resources; and
- upholding the APS Values and the integrity and good reputation of the APS.

Employees are prohibited from releasing official information without proper authorisation. Those with access to national security and other sensitive information have a responsibility to protect that information.

Employees are also responsible for protecting the privacy of individuals with whom they have official dealings.

Employees are reminded that accessing online social media and/or online social networking services from workplace computers, for non-work related matters, is prohibited under the Information Security Policy and is a breach of the APS Code of Conduct regarding the use of Commonwealth Resources.

3. Employee obligations and responsibilities under the APS Values and Code of Conduct when using online social media and/or online social networking services for personal use

Customs and Border Protection employees are obliged by the Code of Conduct to, at all times, behave in a way that upholds the APS Values and the integrity and good reputation of the APS. Users of online social media and/or online social networking services should not identify themselves or others (or enable someone to be reasonably identified) as Customs and Border Protection employees. Any employee participating online must take special care to ensure that any personal postings or blogs cannot be seen to represent the views of the Agency, and do not contain any material that may potentially bring the Agency or the APS in general into disrepute. Employees should remember that online social media and online social networking websites are public forums, and criticism of an APS agency or the Government of the day on such sites could put employees at risk of breaching the Code of Conduct.

There are particular risks associated with participating online. The speed and reach of online communication means that it is never certain where the comment might end up or who might read it. Material posted online effectively lasts forever, may be replicated endlessly, and may be sent to recipients that were never expected to see the post, or who may view it out of context. Even if the employee's participation in online social media is thought by the employee to be anonymous, the obligation to behave in a way that upholds the APS Values and Code of Conduct remains.

Useful questions to consider when participating online include:

- How would Customs and Border Protection's clients and other stakeholders, including the government, the opposition, independents and smaller parties regard the comments were they to read them?
- Would the comments cause stakeholders and members of Parliament to lose confidence in the employee's ability to work in an impartial and professional manner?
- Would posting material of this kind be likely to lower or undermine the reputation of the APS as a whole or Customs and Border Protection individually?
- Could the posting provide foreign agencies or criminal groups with intelligence or information about the operational capacity of Customs and Border Protection?
- Are these comments in line with how the community in general expects the public service to operate and behave?

Use of personal devices such as tablets (eg iPads) and smart phones to participate privately in online social media during working hours must be limited and reasonable, and should not impact on the employee's productivity.

4. Examples of use by APS employees that may be considered inappropriate or unacceptable

The following is a selection of examples of use that may be considered inappropriate or unacceptable - it is **not** an exhaustive list:

- Unauthorised discussion of any Agency-related information – e.g. current operations, policy development, seizures, day-to-day work, matters before the courts, etc. This could be considered misuse of official information and may result in criminal proceedings.
- Unauthorised discussion of any operational or legal matters in which Customs and Border Protection is materially involved (eg joint operations or support, etc).
- Unauthorised comment or information dealing with the infrastructure, hardware, software, security, etc of Customs and Border Protection's IT systems.
- Making personal comments or expressing opinions that could be misconstrued as official comments – e.g. expressing opinion on proposed or current policy.
- Personal attacks on Customs and Border Protection employees, or on clients or employees from other APS agencies – e.g. belittling or making fun of a colleague or client, or engaging in any type of behaviour which could be considered bullying or harassing either directly or indirectly.
- Posting unauthorised photos or video-clips of Customs and Border Protection activities, or of people who can easily be identified as Customs and Border Protection employees (ie colleagues in uniform), regardless of the subject of the photo or video-clip – e.g. posting personal photos or video footage of a seizure.
- Posting any material subject to copyright (eg logos, crests, insignia, etc) without express permission.
- Posting of any Customs and Border Protection email address, telephone number or other contact details.

5. Potential consequences of inappropriate or unacceptable use

Customs and Border Protection employees should be aware of the potential impact that inappropriate or unacceptable use of online social media and/or online social networking sites could have on their employment. This could include:

- Loss of security clearance or a negative Organisational Suitability Assessment (loss of essential qualification or breach of condition of employment)
- Criminal charges and prosecution under the Crimes Act 1914
- Sanction(s) under the APS Code of Conduct (including from complaints of bullying and/or harassment)

Any of the above could lead to termination of employment under section 29 of the *Public Service Act 1999*.

6. Privacy considerations

There are privacy risks associated with using online social media and/or online 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.

For further information, on the potential risks of social media and how to protect your privacy, visit the Office of the Privacy Commissioner (www.privacy.gov.au), the Australian Communications and Media Authority (www.acma.gov.au), or www.staysmartonline.com.au. These websites have information about how to minimise the risks of online activity.

Related Policies and References

Practice Statements:

- Procedures for determining breaches of the Code of Conduct
- Acceptable Use of the Customs and Border Protection Internet Services
- Digital and Online Content Governance

Other Instructions & Guidelines

- Ethics and Standards of Conduct
- Access and Disclosure of Classified Information

Legislation

- *Public Service Act 1999*
- *Public Service Regulations 1999*
- *Privacy Act 1988*
- *Crimes Act 1914*

Other

- APSC Circular 2009/6

Key Roles and Responsibilities

The policy owner for this Instruction and Guideline is the National Director, People and Place.

The advisors to this policy are the Director Employee Conditions, People and Place Strategy and Policy Branch, and team.

Consultation

Internal

- Customs and Border Protection Legal Services Branch
- People and Place representatives
- Work area representatives

BCS CLASSIFICATION: **Pers_Policy_Social Networking**

FILE NUMBER: 2010/055266-01

Approval

Approved on	13 January 2012	
By	A/g Rosemary Holloway National Director People & Place	
Review Period	In line with the Enterprise Agreement cycle	

BCS CLASSIFICATION: **Pers_Policy_Social Networking**

FILE NUMBER: 2010/055266-01