Australian Government
Department of Immigration and Border Protection

File No. 2015/008312-01

Responsible use of social media and corporate electronic communication

Instruction and Guideline

Published date:	1 July 2015
Availability:	Internal
Purpose:	To inform Department of Immigration and Border Protection (the Department) employees of their obligations and responsibilities when using online social media, online social networking and corporate electronic communication, including email, instant messaging and online forums.
Owner:	First Assistant Secretary Integrity, Security and Assurance Division
Category:	Corporate
Sub-category:	Leadership and Workforce
Contact:	Director Values, Policy, Training and Communication Integrity and Professional Standards Branch

Contents

Summary of main points

This Instruction and Guideline outlines:

- definitions of online social media, online social networking services and corporate electronic communication
- obligations and responsibilities when using social media and/or online social networking services in the course of employment and in a private capacity
- obligations and responsibilities when using corporate electronic communication tools, such as email, instant messaging and online platforms
- examples of inappropriate or unacceptable use of social media, social networking and official email, instant messaging and online platforms
- potential consequences of inappropriate or unacceptable use
- privacy considerations.

This Instruction and Guideline applies to departmental employees which includes:

- ongoing and non-ongoing Australian Public Service (APS) employees in the Department of Immigration and Border Protection (the Department)
- the Secretary of the Department and the Australian Border Force Commissioner
- Australian Public Service (APS) secondees to the Department.

Introduction

Departmental employees who participate in social media and social networking, either in the course of their employment or privately, must ensure their behaviour does not conflict with their responsibilities as a departmental employee. This applies equally to the use of departmental email, instant messaging and online platforms. These responsibilities include behaving in a way that is consistent with the APS Values and the integrity and good reputation of the Department and the APS.

From an integrity risk perspective, online social media activities can also expose departmental employees to targeting by organised crime groups. Organised crime groups may target departmental employees in order to gain knowledge or access information or systems for the purposes of circumventing border controls, which is a valuable capability for crime groups. Information posted on social media sites may be used by criminals to gather information on departmental employees, their families, friends and associates in an attempt to identify those who may be susceptible to corruption and groomed for this purpose. Other groups, including lobby groups, may also have an interest in identifying and targeting Departmental employees through social media.

Departmental employees should not rely on site security settings for a guarantee of privacy as material posted on social media sites can easily and quickly be copied and reproduced elsewhere. The terms and conditions of many social media sites include provisions that any postings (including comments, photos and videos) become the property of the site and allow any material posted to be reused or reproduced on other sites. Departmental employees should assume that their identity and the information they post will be revealed more widely. Any information relating to employment that is posted online (including naming an employer or describing a professional role or responsibility) is able to be located quickly and easily by a search engine. Inappropriate use of social media, social networking services or official email, instant messaging or online platforms can compromise Departmental employees (and potentially their family and friends) as well as jeopardise their career. It can also compromise the reputation of the Department.

Scope

This Instruction and Guideline covers the use of social media, social networking services, and official departmental email, instant messaging and online platforms as defined below.

1. Definitions

Social media - online social media can take many forms, including (but not limited to) online social networking services, chat rooms, social blogs, wikis, podcasts, internet forums, gaming and dating sites. Social media includes any website or application that allows users to post dialogue, pictures and/or video (e.g. YouTube) and includes technologies such as picture-sharing. Although not normally defined as social media, the provisions in the policy also apply to the use of personal email and personal instant messaging.

Social networking service - 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, LinkedIn, RSVP, YouTube, Twitter, Snapchat, Instagram, email, Plaxo, Flickr, Friends Reunited, Flixster, Last.fm, Xanga, Meetup, Bolt, MEETin and Tumblr are some examples of online social networking services, however, there are many others.

Corporate electronic communication - official email, instant messaging (e.g. Lync) and online platforms (e.g. Jam) originating from the Department's Information Communications Technology (ICT) environment which carry an official unique source identifier. Unique source identifiers include, for example, border.gov.au and other official domains such as mbc.gov.au and mara.gov.au.

2. Obligations and responsibilities

Using social media in the course of employment

Departmental employees have an obligation to protect official information and electronic information environments, including ICT. Departmental employees are prohibited from releasing official information without authorisation and must abide by policies relating to clearance of material for public release.

The limited circumstances in which departmental employees may be authorised to use certain social media and networking sites and services from workplace computers are set out in relevant departmental policies.

When making comments in an official capacity, departmental employees are bound by the APS Values and Code of Conduct. This includes the obligation under Public Service Regulation 2.1 not to disclose certain information without authority, and obligations for Commonwealth officers under section 70 and 79 of the *Crimes Act 1914*. Departmental employees are also bound by part 6 of the *Australian Border Force Act 2015* (ABF Act) relating to secrecy and disclosure. Departmental employees who are specifically authorised to use social media in an official capacity as part of their departmental role must ensure that any postings they make, or work they undertake, reflect:

- the apolitical character of the APS
- the requirement for departmental employees to act honestly, professionally, and with respect and courtesy.

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

Departmental employees must be specifically authorised to post information on social media and social networking sites and services in the course of their employment. For example, only authorised officers may post information on the Department's websites, the Australian Government Directory, the Migration Blog and official Twitter, Facebook, YouTube, Flickr, LinkedIn, and Instagram. Information or images must have official authorisation for use and, where appropriate, the consent of the Departmental employee whose information or image is disclosed.

In certain limited circumstances, departmental employees may be authorised by a Senior Executive Service (SES) officer to use professional networking sites or services (e.g. LinkedIn) for official purposes.

Departmental employees are permitted to like, follow and comment on official social networking posts in a personal capacity but, in doing so, must not identify themselves as an employee of the Department.

Using social media for private purposes

Use of private personal devices (such as tablets and smart phones) to participate privately in online social media during working hours must be limited and incidental, and should not have an impact on productivity.

APS employees are obliged at all times (including when using social media in a private capacity) to behave in a way that is consistent with the APS Values, and the integrity and good reputation of the APS, including treating others with courtesy and respect at all times. This applies whether the employee is making comment under their own name or a pseudonym.

When acting in the course of their duties, APS employees must be apolitical. Privately, APS employees may express opinions and take part in the political life of their communities. However, employees must be mindful that they do not behave in a manner that suggests they cannot act apolitically or impartially in their work.

If you make public comment in a private capacity, you must not make a comment that is or could be perceived to be:

- Being made on behalf of the Department or the Australian Government, rather than an expression of a personal view.
- Compromising your capacity to fulfil your duties in an unbiased manner.
- So harsh or extreme in its criticism of the Australian Government, a member of Parliament from another political party, or their respective policies, that it raises questions about your capacity to work professionally, efficiently or impartially. Such comment does not have to relate to the employee's area of work.
- So strong in its criticism of an agency's administration that it could seriously disrupt the workplace. Employees are encouraged to resolve concerns by discussion with a manager or by using internal dispute resolution mechanisms, or making a report under the *Public Interest Disclosure Act 2013*.
- A gratuitous personal attack that might reasonably be perceived to be connected with your employment.
- Unreasonable criticism of an agency's clients or other stakeholders.
- Compromising public confidence in the Department or the APS.
- So disrespectful about other departmental employees that the comments constitute bullying or harassment.

When using online social media and/or social networking services in a private capacity, users must not identify themselves or others or enable someone to be reasonably identified as a departmental employee. Departmental employees must avoid using corporate identifiers, including an official email address, user ID or departmental passwords, to register or gain access to online social media and networking services for private purposes. You may, however, choose to identify yourself online as working for the APS.

When using social media or social networking services in a private capacity, departmental employees must not make any comments or postings (including images) about their official duties.

When considering whether to make comment in an unofficial capacity, employees should also reflect on the following questions:

- Could the posting provide foreign agencies or criminal groups with intelligence or information about the operational capacity of the Department?
- Could the comments reasonably cause the Department's clients and other stakeholders, including members of Parliament, to lose confidence in your ability to work in an impartial and professional manner?
- Would a comment of this kind, without proper justification, be likely to lower or undermine the reputation of the Department or the APS as a whole?
- Are the comments in line with how the Australian community in general expects the Department and the APS to operate and behave?
- Are these comments lawful? For example, do they comply with anti-discrimination legislation and laws relating to defamation? Could they involve a breach of secrecy obligations (such as part 6 of the ABF Act, section 91.1 of the *Criminal Code Act 1995*, or sections 70 or 79 of the *Crimes Act 1914*)?

SES employees and social media

SES employees have a special responsibility under section 35 of the *Public Service Act 1999* to promote the APS Values and compliance with the Code of Conduct by personal example and other appropriate means within the Department.

SES employees should be particularly aware that making public comment provides more scope for conflict, real or perceived, between a personal view and:

- their ability to fulfil current and potential duties in an apolitical, impartial and professional manner
- their ability to be responsive to the Australian Government.

3. Privacy and use of social media and social networking

Privacy considerations

There are serious privacy risks associated with using online social media and/or online social networking services. These sites have varying levels of security and all are vulnerable to security breaches.

Before posting or sharing personal information about yourself or others, remember that giving out information online makes it easier for people to gather information for their own purposes.

If you are using smartphones or tablets to take pictures and access social networking sites, you could be inadvertently posting the exact geographic location of your home or daily travel patterns. This technology is known as geotagging. Many phones, tablets and digital cameras are set up to geotag by default.

Departmental employees are encouraged to turn off the geospatial tracking capability on smart devices, including tagging of images, as this can present a very real risk to operations. Criminal

entities may use your location at a particular time as a source of information to be used against you or the Department.

For further information on the potential risks in using social media and how to protect your privacy, visit the Office of the Australian Information Commissioner (www.oaic.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.

4. Acceptable use of corporate electronic communication tools

Official email systems are provided for business purposes and must be used appropriately. Email use must comply with relevant departmental policies. This includes ensuring that information contained in, or attached to emails, is shared on a need to know basis, and is appropriately classified, stored and retained.

When using official email, instant messaging or online platforms, departmental employees must adhere to the principles set out in the APS Code of Conduct and act in a responsible and respectful manner, consistent with the APS Values.

Limited personal use of both private and official email and instant messaging is permitted, provided it is occasional and appropriate in the context of the duties of the departmental employee. Information stored on, sent or received through official email, instant messaging and online platforms, is considered to be the property of the Department and will be retained and managed in accordance with relevant legislation and policies. Usage and content of these systems is also monitored to ensure it is used in accordance with relevant legislation and policies.

5. Inappropriate or unacceptable use of social media, social networking sites or corporate electronic communication

Examples of inappropriate or unacceptable use

The following (non-exhaustive) list provides examples of use that is considered inappropriate or unacceptable:

- Unauthorised discussion of any agency-related information (e.g. current operations, policy development, detentions, seizures of goods, day-to-day work or matters before the courts). This could be considered misuse of official information and may result in criminal proceedings as well as action under the APS Code of Conduct.

- Unauthorised discussion of any operational or legal matter in which the Department is materially involved (e.g. joint operations or support).
- Unauthorised comment or sharing of information relating to the infrastructure, hardware, software, security etc. of departmental systems.
- 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 Department and the government of the day).
- Using official email to send personal messages to public figures or organisations on matters relevant to the Department or the Australian Government.
- Personal attacks on departmental employees, 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.
- Posting or sharing unauthorised photos or video-clips of departmental activities, or of yourself or people who can be identified as departmental employees (e.g. colleagues in uniform, footage of a seizure of goods or visa compliance activity). This includes identifying current work locations.
- Posting or sharing any material subject to copyright (e.g. logos, crests, insignia, without express permission).
- Unauthorised posting or sharing of any official email address, telephone number or other contact details (e.g. it is acceptable to provide your work phone number to your children's school, but it is not acceptable to post your work phone number on your personal Facebook page).
- Using official email for personal gain (e.g. running or supporting a personal business).
- Using another departmental employee's login credentials, or accessing their unlocked computer, to access, delete distribute or convey information.

6. What happens if this Instruction and Guideline is not followed?

Departmental employees are reminded that Instructions and Guidelines have the effect of being directions of the Secretary under the *Public Service Act 1999*. Departmental employees must therefore comply with the requirements of this Instruction and Guideline. A failure, neglect or refusal to adhere to the Instruction and Guideline may give rise to a breach of the Code of Conduct in the *Public Service Act 1999*, the duties of officials under the *Public Governance, Performance and Accountability Act 2013*, an offence under the *Criminal Code Act 1995*, and may result in disciplinary or other appropriate action being taken commensurate with the circumstances and the seriousness of the occurrence.

7. Related policies

- Media Procedures Instruction and Guideline
- Conflict of Interest Instruction and Guideline

8. Legislation and other references

- *Australian Border Force Act 2015*
- *Public Service Act 1999*
- *Public Service Regulations 1999*
- *Privacy Act 1988*
- *Freedom of Information Act 1982*
- *Crimes Act 1914*
- *Public Interest Disclosure Act 2013*

9. Other

- APSC Circular 2012/1: Revisions to the Commission's guidance on making public comment and participating online

10. Consultation

Internal consultation

The following internal stakeholders have been consulted in the development of this Instruction and Guideline:

- Integrity, Security and Assurance Division
- Communication and Media Branch
- Legal Division
- Procurement
- all staff through Department-wide consultation.

External consultation

The following external stakeholders have been consulted in the development of this Instruction and Guideline:

- Australian Public Service Commission
- staff representatives through the National Staff Consultative Forum
- Community and Public Sector Union.

11. Endorsement

Endorsed on	29 June 2015	Signed
By	Kaylene Zakharoff Assistant Secretary Integrity and Professional Standards	

12. Approval

Approved on	29 June 2015	Signed	
By	Jan Dorrington First Assistant Secretary Integrity, Security and Assurance		
Period of Effect	3 years from 1 July 2015	Review Date	1 July 2016

Australian Government
Department of Immigration and Border Protection

July 2015

Fact sheet

Responsible use of social media and corporate electronic communication

What is meant by 'social media'?

Social media is any website or application (app) that allows you to post dialogue, share pictures, video, email and/or messaging.

Common social media sites include Facebook, YouTube, LinkedIn, Instagram, Twitter and Snapchat but also include instant messaging services such as forums, blogs, dating sites and mobile social networking apps.

What is meant by 'corporate electronic communication'?

Corporate electronic communication refers to any type of technology provided by the Department of Immigration and Border Protection (the Department) that allows you to communicate electronically with other people. This includes your departmental email address, instant messaging (e.g. Lync) and online platforms (e.g. Jam).

What are my responsibilities?

Your obligations are set out in the Department's *Responsible Use of Social Media and Corporate Electronic Communication Instruction and Guideline* (Social Media I&G). Importantly, you:

- Must behave at all times in a way that upholds the Australian Public Service (APS) Values and the integrity and good reputation of the APS, including treating others with courtesy and respect.
- Must not make public comment online that could be perceived to be made on behalf of the Department.

How could my use of social media be a risk to me or my work?

Online activities can expose departmental employees to targeting by organised crime groups. Being able to circumvent border controls is a valuable capability for crime groups.

The information you post on social media sites may be used by criminals to gather information on you, your families, friends and associates in an attempt to identify if you may be susceptible to corruption and groomed for this purpose. The speed and reach of online communication means that you can never be certain who will read your posts or view your photos or other personal information.

Technology today is wide reaching, so it is vital that you are aware of the potential risk to yourself and the Department through your social media use, whether privately or in the course of your duties.

Am I allowed to have personal Facebook, Twitter or other social networking accounts?

Yes, however, your social media use must comply with the Social Media I&G.

Can I identify myself online as working for the Department?

No, you must not identify yourself or a colleague on social media as a departmental employee (unless authorised to do so). However, you may choose to identify yourself as working for the APS. These measures are designed to protect you by limiting the opportunity for you to be identified and groomed through your social media use.

What is considered inappropriate use of online social media and social networking?

Inappropriate use includes (but is not limited to):

- unauthorised posts that contain:
  - agency-related information
  - information about operational or legal matters in which the Department is involved
  - information about the infrastructure, hardware, software, security, etc. of departmental IT systems
  - photos or video-clips of departmental activities, or of people who can easily be identified as departmental employees (e.g. colleagues in uniform)
  - material subject to copyright (e.g. logos, crests, insignia)
  - departmental email addresses, telephone numbers or other contact details
- personal comments or opinions that could be misconstrued as official comments
- personal attacks on departmental employees, clients or individuals from other APS agencies.

What if I post my views anonymously?

You must comply with the Social Media I&G at all times—even if you post using an alias or anonymously, you may be identified at a later time.

When you participate in online social networking activities, (privately or in the course of your employment) you must ensure your behaviour does not reflect badly on you, the Department or the Australian Government, now or in the future.

What if I need to use social media during the course of my duties?

If you are authorised to use social media in the course of your employment, you must ensure that any posts reflect:

- the apolitical character of the APS
- the requirement to act honestly, professionally and with respect and courtesy
- the responsibility to protect the privacy of individuals with whom you have official dealings.

You must not release official information unless you are authorised to do so. You have a responsibility to protect classified and personal information.

Can I use my work email for personal use?

Limited personal use of official email is permitted, provided it is occasional and does not interfere with your duties. Information stored on, sent or received through official email, instant messaging and online platforms remains the property of the Department. Usage and content of these systems is monitored to ensure compliance with relevant policies.

Can I use my own personal mobile electronic device at work?

The use of your own personal mobile electronic device, such as a tablet or smart phone, to participate privately in online social media during working hours must be incidental and reasonable, and should not impact on productivity.

What are the consequences for inappropriate use of social media and electronic communications?

Inappropriate use of social media sites or Department provided communication tools can compromise you, your family, friends and colleagues as well as jeopardise your career.

Potential consequences include:

- loss of your security clearance or your Employment Suitability Clearance
- criminal charges and prosecution under the *Crimes Act 1914*
- sanction(s) under the APS Code of Conduct, other professional standards frameworks or under a contract of employment (including from complaints of bullying and/or harassment).

Any of the above could lead to termination of your employment.

Further information

For more information refer to the policy instruction or contact:

Integrity and Professional Standards

Ph: s. 22(1)(a)(ii)

E: s. 22(1)(a)(ii) @border.gov.au

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

BECOMING #SOCIALLY AWARE

These days, social media is ubiquitous. We share stories, keep in touch with family and friends, and build our social and professional networks. As public servants, it's important for us to be aware of the Australian Public Service Commission's guide on making public comment and participating online and the Department's social media policy.

We have the responsibility to ensure our online behaviour is consistent with the APS Values, and the integrity and good reputation of the Department and Public Service. As a result, avoid making public comment about your official duties, and always be mindful of how your online comments may be perceived—think twice before posting.

From an integrity risk perspective, online social media activities can expose staff to targeting by organised crime groups who may use information in an attempt to corrupt staff and circumvent border controls.

Take time to review your social media profiles and remove any information—such as photos, comments, tags and geo-tags—which identifies you or others as working for the Department. Profiles set up using an official email, corporate ID or departmental password must be removed.

The Department's social media team is the only team who has permission to post on behalf of the Department. Any questions or feedback email the Integrity and Professional Standards team.

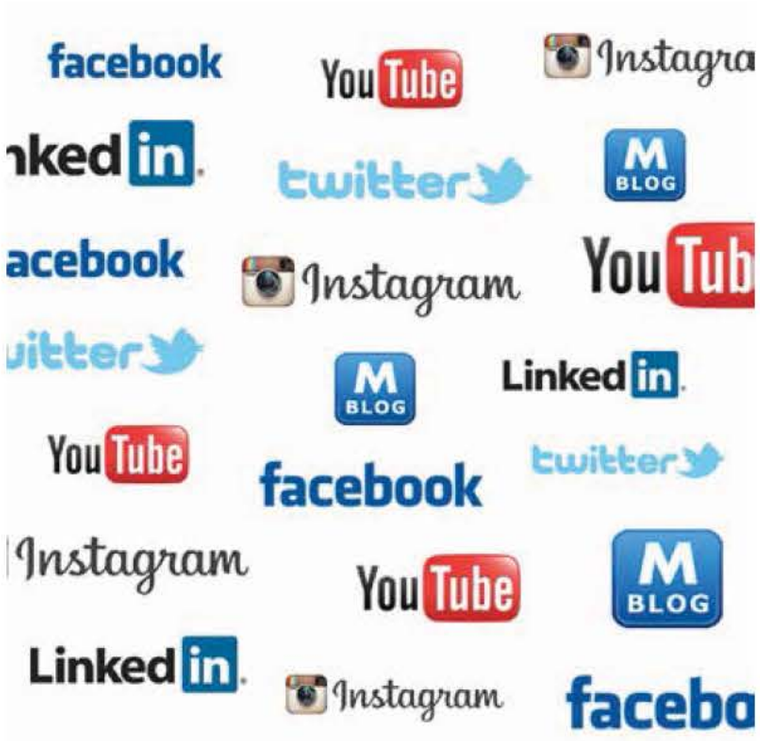

PHOTO: The Department uses YouTube, Facebook, Twitter, Instagram, LinkedIn and the Migration Blog on Govspace to communicate with the public.