Use of Social Media and Other Online Services

Procedural Instruction

Document ID (PPN)	SM-1560
TRIM record number	ADD2023/4972914
BCS function	Technology and Information Management
Document owner	Assistant Secretary Integrity and Professional Standards
Approval date	20 November 2023
Document contact	Integrity Strategy and Policy Section *integrityawareness@homeaffairs.gov.au*

Table of Contents

1. Purpose

This Procedural Instruction (PI) describes your obligations when using social media, including online services, in a personal capacity and on personal devices. The Department of Home Affairs (the Department), which includes the Australian Border Force (the ABF), reminds all Immigration and Border Protection workers (IBP workers) of their obligations that extend outside the work place, including online environments. Under the Public Service Act 1999 (the PS Act), employees are required to display behaviours that are consistent with the Australian Public Service (APS) values, and comply with the APS Code of Conduct. This PI also reminds employees of the risks that social media and online services, presents to the Department, including systems and people.

For many people, social media and online services are a part of daily life. You are permitted to use social media platforms and other online services in a personal capacity, on your personal devices. However limits to what an individual can say and do apply to online environments. The unique nature of APS employment means an employee's expressed views can reflect not only on them as an individual, but on the Department and the APS as a whole. Your personal behaviour can ultimately affect the confidence of the Australian community and the Government in the integrity of the APS as an institution.

When using social media or other online services in a personal capacity, staff must be aware of what they say and do online because:

- foreign intelligence services, organised crime groups and others can (and do) use social media to target government employees – and to research if you could be blackmailed or compromised; and
- there is no guarantee that information posted online will remain secure, or can be removed at a later stage.

2. Scope

2.1. In Scope

This PI applies to all IBP workers and only covers personal use of social media and online services, on personal devices.

If unsure as to whether this PI applies to an employee, please contact integrityawareness@homeaffairs.gov.au.

2.2. Out of Scope

This PI does not apply to the use of Department owned and operated systems to access online and open source information, including social media or other online services, to support operational priorities and projects within the Department's functions and activities. These circumstances are captured in other policies and procedures.

This PI does not cover strategies for employees to manage their own personal safety and cyber security risks when using the internet. For information on how to manage these risks, visit www.cyber.gov.au.

This PI also does not cover circumstances captured in the Department's other policies and procedures regarding:

- The use of:
    - the Department's official ICT systems including departmental email and instant messaging services (refer to Acceptable use of Departmental ICT Systems and Information – PI (HR-3320) ;

- the Department's official social media and other online services (refer to the Social Media intranet page or contact Media and Communications Branch at socialmedia@homeaffairs.gov.au); and
- social media and other online services for the purposes of performing official duties (refer to the Online Open Source and Social Media Access Policy – PS (TI-1214), as well as relevant local work area policies and procedures);

- An employee's obligations to:
  - comply with their legal obligations regarding the secrecy, use, access and disclosure of certain kinds of information, as well as any associated obligations under any relevant Memoranda of Understanding and departmental policies and procedures. For further information, see the Secrecy and Disclosure intranet page, check the Policy and Procedure Control Register for policies that may be relevant to them and/or contact privacy@homeaffairs.gov.au;
  - report all Declarable Circumstances – PI (SM-1552) (including changes relating to social media usage) to Integrity and Professional Standards Branch;
  - declare (and work with the Department to manage) Conflict of Interest – PI (SM-1556) and Declarable Associations – PI (SM-1551) (including relationships and associations that occur through your social media usage);
  - complete a Security Incident Report relating to unusual activity or inappropriate advances/requests while using social media or other online services – or if classified or official information is observed on the internet that may have been unlawfully released. For further information, see the Security Event Reporting intranet page or contact Security Branch at security@homeaffairs.gov.au or 1300 484 987; and
  - report suspected breaches of departmental policies and procedures that may amount to serious misconduct, fraud or corruption, to Integrity and Professional Standards Branch. For more information see the Reporting Integrity Issues intranet page or contact Integrity and Professional Standards at integrity@homeaffairs.gov.au or 1800 277 872.

2.2.1. Official Departmental Social Media

This PI does not apply to the official use of the Department's own social media platforms.

Employees may appear on official departmental social media accounts and may be identifiable as departmental employees. The Department's Social Media Team will make efforts to limit personal details published online to reduce identifying particulars (for example, use of first name only, quote an individual's position rather than name). Official content can only be published by the Department's Social Media Team with consent of the member featured, approval from the relevant line area Director, as well as approval from Director, Media and Communications Branch.

3. Obligations when using social media and online services in a personal capacity

3.1. Standards of behaviour

The unique nature of APS employment means expressing your views can reflect not only on you as an individual, but on the Department and the APS as a whole. Personal behaviour can ultimately affect the confidence of the Australian community and the Government in the integrity of the APS as an institution.

This is why some of our obligations as public servants extend into our private lives, and must be balanced with our rights as citizens.

All APS employees are bound by the APS Values, Employment Principles and Code of Conduct in the PS Act. These obligations set high standards of behaviour for individual public servants, with the ultimate purpose of maintaining public confidence in the integrity of public administration.

Your obligations under the Code of Conduct is to behave at all times in a way that upholds the APS Values and Employment Principles, and the integrity and good reputation of our agency and the APS.

This means that your behaviour outside work is subject to the Code of Conduct to the extent that:

- it could reasonably be viewed as failing to uphold the integrity and good reputation of the Department or the APS; and/or
- it could reasonably call into question the their capacity to comply with the APS Values and Employment Principles in their work - for example, their capacity to be impartial or respectful.

Your personal behaviour on social media and online services can breach the Code of Conduct. The higher the risk that a post could undermine trust in the APS, the more likely it is to be inconsistent with the Code of Conduct. Section 4.3 outlines how you can meet these obligations in practice.

You must meet these standards of behaviour while you are both on and off duty, even if you are using social media and online services:

- under a false name such as an alias or pseudonym; and/or
- through a joint, private and/or anonymous account.

3.1.1. Social Media and Professional networking and associations

Your obligations as an APS employee includes the requirement that you do not specifically identify yourself as an employee or an associate of the Department when using social media or other online services in a personal capacity. This extends to professional networking platforms, such as LinkedIn. This is particularly the case if you have a unique or uncommon name which may increase the likelihood of your personal online activities and profiles being identified and linked to the Department.

While it is not encouraged by the Department, should an employee choose to do so, you can identify yourself as being employed by (or associated with) the ‘Australian Government’. If you choose to do so, you should exercise an additional degree of caution about what you say and do online. Public identification as an employee or associate of the Australian Government can increase the likelihood of your online activities being monitored or targeted by foreign intelligence services, organised crime, the media, general public and others. This can increase personal risks, as well as risks to the Department and the Government.

In some cases, you may need to disclose your employer to a professional association for membership purposes. Certain professional associations (such as a Law Society) may also publish this information online. Where you are required to be a member of a professional association in order to perform your duties/undertake your role with the Department, such publication is acceptable. Refer to 4.1.5 for information specific to Senior Executive Staff (SES) employees.

3.1.2. Conduct that is not permitted

If you use social media or online services, you also need to ensure that you do not:

- Post any material:
    - identifying yourself as being employed by (or otherwise associated with) the Department;
    - that could enable someone to determine that you are employed by (or otherwise associated with) the Department;

  - containing details of official departmental email addresses or contact details;
  - containing details of any official departmental business including current operations, policy development, detentions, seizures, day-to-day work or matters before the courts;
  - containing material subject to copyright (such as the Department's or Australian Government's logos, crests or insignia);
  - such as photos of you or others wearing an official lanyard and/or uniform; and/or
  - such as photos of you at departmental events or premises.
- Accept friend requests or add as a contact or associate with:
  - anyone who is a departmental client that you have met in an official capacity (for example, a client whose visa you have assessed);
  - anyone you know or reasonably suspect is involved in (or has previously been involved in) criminal or illegal activities;
  - anyone you know or reasonably suspect is currently (or was previously) in immigration detention; and/or
  - anyone who is an immediate family member of anyone detailed above.
- Comment on any posts (including within online messaging services):
  - about colleagues, clients or partner agencies in any way that is critical, demeaning or disrespectful; and/or
  - about the Department or the Australian Government and its policies and officers in any way that is overly critical or harsh.
- support, like, share or otherwise associate yourself with any extremist ideology such as supporter sites for Islamic State or white supremacist and neo-Nazi groups;
- join, create, administer or otherwise participate in group chats or platforms that are aligned with extremist ideologies; and
- use individual work email address when subscribing to social media or professional networking associations.

For further guidance, refer to Attachment D - Practical Examples, as well as the following Australian Public Service Commission resources:

- Personal behaviour on social media: Guidance for APS employees and agencies;
- APS Values and Code of Conduct in practice and in particular Section 6: employees as citizens; and
- Comcare v Banerji.

3.1.3. Individuals whose information is already in the public domain

In certain cases, information about an employee such as their photograph, name and rank/title may already be in the public domain. For example, this information may have been published online if an employee:

- has participated in authorised media engagement activities;
- has attended conferences or professional networking events;
- was the contact officer for recruitment or procurement related activities;
- is recorded on an official Australian Government public directory or Gazette;
- has been a subject or witness in court proceedings; and/or

- appeared on a Border Security episode.

Even in these circumstances, your obligations outlined under section 4.1 continue to apply.

3.1.4. Online underground platforms (commonly known as the 'dark web')

Employees should not access underground platforms, to limit the risk to themselves and departmental information and assets. Online underground platforms - or 'dark web' forums - can be used by cyber criminals to facilitate criminal activity and pose additional risks to more public platforms. Employees who choose to engage in these forums have an increased risk being targeted by criminal entities seeking access to departmental security, data and or systems, including through blackmail and corruption.

3.1.5. Additional obligations on Senior Executive Service (SES) employees

The Department acknowledges SES are public figures through the nature of their work, and are listed in the Australian Government Directory as employees of the Department. As such, SES employees are permitted to identify themselves as working for the Department on their LinkedIn profile; however, they are reminded of their ongoing responsibilities and obligations when sharing comments or personal views online. Where possible, SES employees should list their employer as 'Australian Government', rather than the Department.

SES employees have a particular responsibility when using social media and other online services in a personal capacity because they:

- can influence the relationship between stakeholders and government;
- are likely to be required to advise on, or lead, the implementation of government policies and programs within agencies and across agency and portfolio boundaries; and
- are required by personal example to promote the APS Values and compliance with the Code of Conduct.

If you are an SES employee, you should give careful consideration to how your online activities could be perceived, as you are likely to attract an additional degree of scrutiny from the media and general public.

3.2. Making public comment on social media

The Department respects employees' freedom to participate in Australia's democratic processes. In your personal time you are free to:

- like, share, follow and comment on official departmental social networking posts
- make public comment in an unofficial capacity (including on official departmental social networking posts), as long as:
    - their comments are lawful (for example, they have not unlawfully disclosed information, their comments do not breach anti-discrimination legislation and/or their comments are not defamatory);
    - they are clear to readers that they are expressing their own views; and/or
    - they do not say or do anything that would cause a reasonable person to conclude that they or the department are unable to serve the Government of the day impartially, apolitically and professionally.

It is a good idea to include a statement on your social media platforms, or in individual posts if necessary, to the effect that your views do not represent those of your employer. However, this will not necessarily protect you from a finding that you have breached the Code of Conduct.

For example, if an employee chooses to publish material that is discriminatory, a disclaimer of this kind will not protect them from a Code of Conduct investigation. People who read that material may reasonably be

concerned as to whether someone with opinions like these can genuinely serve the public and the government as an impartial and professional public servant. Such statements may even affect the reputation of the Department and the APS.

Employees should also consider whether the nature of the content they are posting could give rise to unintended security risks. For example, posting pictures of themselves inside a departmental building. The resulting photo provides data about where they are, what the building lay out is and their daily routines – all of which can create security risks if used inappropriately.

3.3. How to meet these obligations in practice

The Department expects that you will exercise your judgement and common sense when using social media and online services in your personal capacity considering whether your actions meet your obligations under the APS Values, Code of Conduct and Employment Principles. As a guiding principle, you should consider the following before doing anything online:

- if you would not say something in person, then you should not say it online
- if you are unsure about whether a post may be inappropriate or could be misinterpreted, you should not post the material online
- how your actions would look to:
    - friends, family and colleagues;
    - partner agencies (such as the Australian Federal Police);
    - members of the public and general community (the 'pub test'); and/or
    - the media (the '7:30 report test').
- whether your actions will cause harm to another person or their reputation;
- whether the data you are disclosing could give rise to security risks; and/or
- whether you are lawfully permitted to disclose the information.

3.4. Response to inappropriate online conduct

If the Department becomes aware that an employee's online conduct represents a code of conduct breach, the Integrity and Professional Standards Branch will consider the nature of the breach and whether an investigation or referral to other relevant stakeholders is required. Some of the responses available to the Department include, but are not limited to:

- informal management action. For example, counselling conducted by an employees' direct supervisor;
- training including re-familiarisation with this PI;
- conducting an investigation to determine whether the conduct has breached the APS Code of Conduct;
- conducting an investigation to determine whether a security breach has occurred;
- referring the matter to investigative agencies such as the National Anti-Corruption Committee, Australian Federal Police or the Director of Public Prosecutions;
- referring the matter to professional bodies such as law societies or the Medical Board of Australia; and
- referring the matter for additional personnel screening including in relation to an Employment Suitability Clearance and/or Australian Government Security Vetting Agency Security Clearance.

3.5. Reporting inappropriate online conduct

A key component of the Department's Integrity Framework is the requirement that IBP workers have the responsibility to report any suspected breaches of this policy, including any online conduct that may represent a code of conduct breach. This is known as mandatory reporting. If you become aware of another employees online conduct and you believe it represents a code of conduct breach, you must make a report as soon possible. Mandatory reports can be made either verbally or in writing.

How to make a mandatory report

An IBP worker can submit a mandatory report to Integrity and Professional Standards Branch using any of the following channels:

- Integrity referral form (bcz.gov.au);
- by phone: 1800 277 872;
- by email: integrity@homeaffairs.gov.au; or
- by post: Integrity and Professional Standards Branch, PO Box 25, Belconnen, ACT, 2616.

For more information on reporting, please refer to on the Department's Mandatory Reporting – PI (SM-1557).

4. Statement of Expectation

The APS Code of Conduct states that an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction under subsection 13(5) of the *Public Service Act 1999* (the Public Service Act).

Failure by an APS employee to comply with any direction contained in this Procedural Instruction document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions under subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the *Australian Border Force Act 2015*, (the ABF Act) requires all IBP workers who are not employed under the Public Service Act to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in this Procedural Instruction document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

All IBP workers who make decisions or exercise powers or functions under legislation have a duty to do so in accordance with the requirements of the legislation and legal principles.

5. Accountability and responsibility

Role	Description
Immigration and Border Protection Worker (IBP) workers	Have a responsibility to read and understand this document. Have a responsibility to use social media and other online services in a responsible manner in line with this PI and the *APS Values, Code of Conduct* and *Employment Principles*.

Role	Description
	Have a responsibility to report any suspected breaches of this policy to Integrity and Professional Standards Branch.
Supervisors and managers	Have a responsibility to read and understand this document. Have a responsibility to use social media and other online services in a responsible manner in line with this document and the *APS Values, Code of Conduct* and *Employment Principles.* Have a responsibility to assist staff to understand their obligations in regards to this policy and how to use social media and other online services in a responsible manner. Have a responsibility to immediately take reasonable management action in relation to staff engaging in suspected non-compliance with this policy. This may include supervisors and managers calling out inappropriate behaviours as and when they become known, asking staff to comply with this policy and reporting the matter and their actions to Integrity and Professional Standards Branch. Have a responsibility to report any suspected breaches of this policy to Integrity and Professional Standards Branch.
Senior Executive Service (SES) employees	Have a responsibility to promote compliance with the *APS Values, Code of Conduct* and *Employment Principles* including this PI – including leading by personal example.
Integrity and Professional Standards Branch (I&PS)	Administers and maintains this PI and related documentation. Receives referrals and makes assessments about Integrity related matters that relate to serious breaches of this PI.

6. Version Control

Version number	Date of issue	Author(s)	Brief description of change
1.0	July 2019	C Vaughan	Draft
2.0	September 2019	K Ryan	Draft
3.0	September 2019	A Herak	Review and editing
4.0	September 2019	K Ryan	Draft
4.1	October 2019	C Gardiner	Updated draft

Version number	Date of issue	Author(s)	Brief description of change
4.2	January 2020	C Gardiner	Revised structure and incorporation of comments from stakeholders within I&PS Branch
4.3	February 2020	M Henderson	Revised to include additional feedback
4.4	March 2020	C Gardiner	Final draft
4.5	April 2020	C Gardiner	Incorporation of comments from Legal Group
4.6	August 2023	P Pavez	Revised structure and incorporation from stakeholders within Legal Group and Cyber Risk Services. Inclusion of: - online underground platforms, official departmental social media and updated LinkedIn information for SES identifying on social media and online service. - response to and reporting inappropriate online conduct, added.
4.7	November 2023	N Boyd	Minor edits

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Australian Public Service Code of Conduct	*Code of Conduct*	The *Code of Conduct* out lines expected behaviours that APS employees must adhere to and can be found here - APS Code of Conduct | Australian Public Service Commission
Australian Public Service Employment Principles	*Employment Principles*	Information on the Australian Public Service Employment Principles can be found here - Employment Principles | Australian Public Service Commission (apsc.gov.au)
Australian Public Service Values	*APS Values*	The *APS Values* articulate the Australian Government's expectations of public servants in terms of performance and standards of behaviour. Information can be found here - APS Values | Australian Public Service Commission (apsc.gov.au)
Immediate Family Member		An Immediate Family Member means: • a spouse, de facto partner, child, parent, grandparent, grandchild or sibling of an individual; • a child, parent, grandparent, grandchild or sibling of a spouse or de facto partner of an individual; and • any other individual or family member (such as a cousin, aunt, uncle, niece or nephew) with which an individual has a close familial relationship that has the same characteristics as a relationship outlined above.
Immigration and Border Protection Worker	IBP worker	Defined in the Secretary's Determination of Immigration and Border Protection Workers and under subsection 4(1) of the ABF Act, includes but is not limited to: • all APS employees in the Department • persons employed by an Agency under the Public Service Act whose services are made available to the Department (often referred to as 'secondees') • persons engaged as consultants or contractors to perform services for the Department in-house in the Department • persons engaged as consultants or contractors to performing services for the Department that require non-public access to Departmental Assets. A complete list of persons who are IBP workers can be found at: 1. subsection 4(1) of the Australian Border Force Act 2015 (ABF Act); and 2. the Determination of Immigration and Border Protection Workers signed 29 June 2015 by Secretary Michael Pezzulo AO.

Term	Acronym (if applicable)	Definition
Online services		Any other website, application or platform that allows for user participation and interaction even if this is not the primary purpose of the website, application or platform. This includes, for example, news, product/service/travel review, shopping or other websites and services.
Personal capacity		Refers to any use of social media or other online services that is undertaken outside of official duties as an IBP worker.
Post		Refers to any shared or created content put on social media. This could be a post on Facebook or content created and edited on Wikipedia.
Social media		Social media includes tools such as websites and applications that allow users to create and share content and to participate in social networking. Generally, social networks are used to share personal information in a combination of comments, messages, photos and/or videos. Social media may include (but not limited to): • social or professional networks, such as Yammer, Facebook and LinkedIn; • media sharing networks, such as Snapchat, Instagram, SoundCloud and YouTube; • messaging services, such as WhatsApp, Signal and Facebook Messenger; • bookmarking and content curation networks such as Pinterest; • blogging networks such as WordPress; • micro-blogging networks such as Twitter; • discussion forums such as Whirlpool; • wikis such as Wikipedia; • online gaming networks such as World of Warcraft (WOW); and • sharing economy websites such as Gumtree and Uber.

Attachment B – Assurance and Control Matrix

1.1. Powers and obligations

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	**Reference (e.g. section)**	**Provision**		
Public Service Act 1999	subs 13 (1) subs 13 (3) subs 13 (5) subs 13 (11)	Section 13 of the *Public Service Act* contains the *APS Code of Conduct*	No	N/A
Australian Border Force Act 2015	subs 55 (1)	The Secretary may give directions to IBP workers in connection with the administration and control of the Department	No	N/A
Privacy Act 1988	Schedule 1	Australian Privacy Principles	No	N/A

1.2. Controls and assurance

Related Policy	• Integrity and Professional Standards Frameworks – PS (SM-6697) • Acceptable use of Departmental ICT Systems and Information – PI (HR-3320) • Online Open Source and Social Media Access Policy – PS (TI-1214) • Records Management Policy – PS (TI-1094)
Procedures / Supporting Materials	• Declarable Circumstances – PI (SM-1552) • Declarable Associations – PI (SM-1551) • Conflicts of Interest – PI (SM-1556) • Performance Management – PI (HR-2193) • Mandatory Reporting – PI (SM-1552) • Protective Security Policy Framework • Secretary Determination of Immigration and Border Protection Workers • Secretary Determination 1 of 2015 – Professional Standards • Secretary Determination 2 of 2015 – Employment Suitability and Security Screening • Secretary Determination 3 of 2015 – Integrity Measures
Training/Certification or Accreditation	The Essentials eLearning

Other required job role requirements	Employment Suitability Clearance Baseline Security Clearance
Other support mechanisms (eg who can provide further assistance in relation to any aspects of this instruction)	Integrity Strategy and Policy Section integrityawareness@homeaffairs.gov.au
Escalation arrangements	Director, Integrity Strategy and Policy Section Integrity and Professional Standards Branch | Integrity, Security and Assurance Division Director of Integrity Strategy and Policy via integrityawareness@homeaffairs.gov.au
Recordkeeping (eg system based facilities to record decisions)	Content Manager (TRIM)
Program or Framework (i.e. overarching Policy Framework or Business Program)	Integrity Framework Policy Statement
Job Vocational Framework Role	All Job Roles

Attachment C – Consultation

1.1. Internal consultation

- Integrity, Security and Assurance Division
- Media & Communications Branch
- Legal Group
- Records Management Section
- Workforce Management and Coordination
- Privacy & Information Disclosure Section
- Freedom of Information Section
- Cyber Risk Services
- PPCF Section
- All Staff

1.2. External consultation

- Community and Public Sector Union.

Attachment D – Practical Examples

Practical example 1

John Sampson is a Marine Tactical Officer in the ABF. He operates a Facebook account where he does not identify himself as an ABF Officer. John's profile name is *John "Skipper" Sampson*. John maintains a 'public' Facebook profile and has posted links to a number of news articles relating to Operation Sovereign Borders including the interception and turn-back of boats. One of John's friends comments on one of John's posts, stating "*mate you and the boys are doing a great job, I know it's hard work for you and the crew while you are at sea but keep it up!*" John then replies to this comment "*thanks mate, has been pretty intense lately, lots of long hours … they haven't breached the borders yet!"*

John is allowed to like and post links to media articles relating to the Department and its operations. However, in this case, John may have breached his obligations as an APS employee because his comments may have disclosed classified and/or sensitive operational information. In addition, John's comments could enable someone to work out that he is employed by the ABF. The correct course of action in this example would be for John to:

- delete his friend's comment;
- not comment himself;
- politely ask his friend to stop referring to his work or position online; and
- reconsider the privacy settings on his Facebook account, including what can be posted by others on his Facebook page.

Practical example 2

James, Sally and Monica are all employees of the Department and operate a WhatsApp group outside of work hours. They use the WhatsApp group to mainly discuss common interests outside of the workplace. Recently, James has started to post messages to the group about his supervisor Brian. James' messages become increasingly critical of Brian, stating "…*Brian is such an idiot, I can't believe someone promoted him to an EL2. What a joke! Seriously what is wrong with this place … he doesn't even know how to write a Minute! Every day I am constantly fixing his mistakes…I'm sick of his incompetence. Yesterday he asked me what a BFORT was – can you believe it! And he came from the ABF!! lol seriously what a load of rubbish!!!!!!!!!…Next time he annoys me I am going to scream :p.."*

Even though the group is using WhatsApp in their own private time, James may have still breached his obligations under the *APS Values* and *Code of Conduct* because he has not treated his colleague with respect and courtesy. In cases such as this, members of private groups can and often do take copies of the chat history and provide these to Integrity and Professional Standards Branch for investigation. Even social media services such as Snapchat are not immune to being captured and circulated outside of those services.

Practical example 3

Susie operates a blog known as *The True Observer*. The blog is run using an alias *@truthseeker*. Susie has not posted anything about who she is or that she is employed by the Department. The domain for her blog is also registered using a privacy protection service.

The purpose of *The True Observer* as stated on the blog is to 'expose the crooked politicians'. She uses the blog to re-post a series of news articles about corruption within the Australian Government. In addition, she writes her own articles on the blog. All articles follow a similar theme alleging that mainstream political parties are corrupt and should therefore be voted out at the next Federal Election. Several current and former Ministers are directly referred to in the articles.

While Susie is engaging in political discourse, her allegations of widespread corruption in all major political parties (including the Department's current Minister) could be seen to be so critical that it may call into question her ability to support the government of the day. It does not matter that Susie is posting this material anonymously.