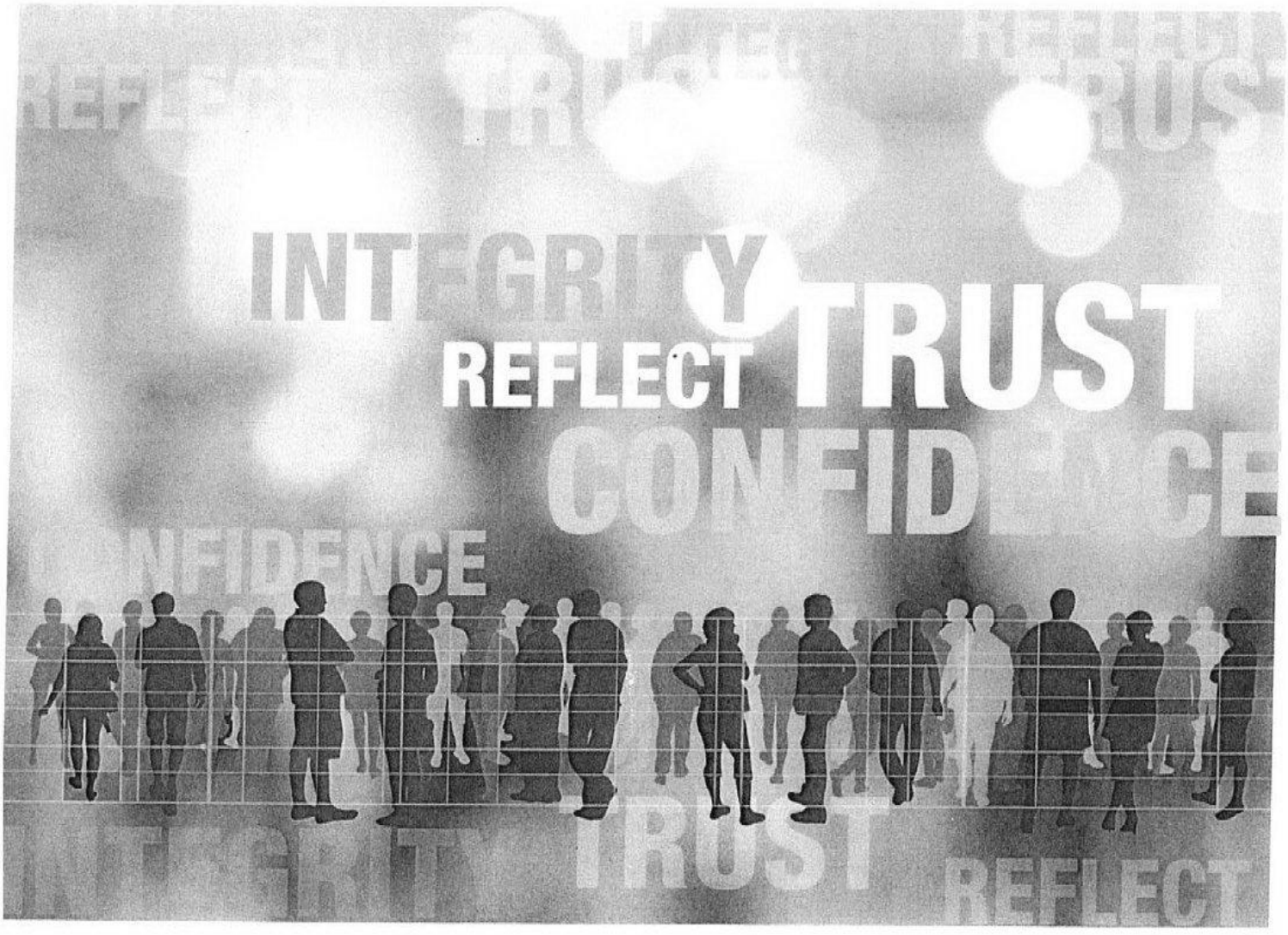
Australian Government

Australian Public Service Commission

APS VALUES AND CODE OF CONDUCT IN PRACTICE



Section 6: Employees as citizens

6.1 Summary

6.1.1 Australian Public Service (APS) employees are citizens and members of the community, but the right to serve the community as APS employees comes with certain responsibilities. These responsibilities include maintaining the confidence of the community in the capacity of the APS, and each member of it, to undertake their duties professionally and impartially.

6.1.2 Section 13(11) of the APS Code of Conduct (the Code) in the *Public Service Act 1999* (PS Act) requires APS employees to behave in a way that upholds the APS Values and Employment Principles in sections 10 and 10A of the PS Act, and the integrity and good reputation of the employee's agency and the APS at all times.

6.1.3 Areas where employees should take particular care about their behaviour as citizens and its impact on their duties include:

a. when considering making public comment in an unofficial capacity
b. when participating in political activities
c. when considering an action that might raise a perception of conflict of interest, such as taking a second job, participating in voluntary activities, accepting a gift or benefit or making an investment—see Section 5: *Conflict of interest*
d. when working overseas—see Section 8: *Working overseas*
e. when they are identifiable as an APS employee.

6.2 Making public comment, including online

6.2.1 The engagement of APS employees in robust discussion is an important part of open government.

6.2.2 Commenting publicly online is becoming increasingly common for APS employees. When doing so, they must ensure that their behaviour at all times upholds the APS Values, Employment Principles and the Code.

6.2.3 The term 'public comment', used broadly, includes comment made on matters of interest, such as:

a. at public speaking engagements
b. during radio or television interviews
c. on the internet including blogs, social networking sites and other online media that allow user participation and interaction
d. in correspondence with the press
e. in books or notices
f. in academic or professional journals
g. in other forums where the comment is intended for, or may be accessed by, the community.

6.2.4 Broadly speaking, APS employees make public comment in two capacities:

a. official—that is, for purposes connected with their APS employment
b. unofficial, including:
    i. where an employee is a subject matter expert independent of their APS role and makes comment in that capacity
    ii. in a private capacity.

Making public comment in an official capacity

6.2.5 Some APS employees, as part of their official duties, provide comment to the media and others in the community about agency activities and government programs. Section 4: *Managing information* describes the legal and regulatory framework that governs the disclosure and use of official information when making public comment in an official capacity.

Making public comment in an unofficial capacity

6.2.6 APS employees may generally make public comment in an unofficial capacity, so long as the comment is lawful and the employee makes it clear they are expressing their own views.

6.2.7 When employees make public comment in an unofficial capacity, it is not appropriate for them to make comment that is, or could be reasonably perceived to be:

a. being made on behalf of their agency or the Government, rather than an expression of a personal view
b. compromising the employee's capacity to fulfil their duties in an unbiased manner—this applies particularly where comment is made about policies and programs of the employee's agency
c. so harsh or extreme in its criticism of the Government, a Member of Parliament from another political party, or their respective policies, that it raises questions about the employee's capacity to work professionally, efficiently or impartially
d. so strong in its criticism of an agency's administration that it could seriously disrupt the workplace—APS employees are encouraged instead to resolve concerns by informal discussion with a manager or by using internal dispute resolution mechanisms
e. a gratuitous personal attack that might reasonably be perceived to be connected with their employment
f. compromising public confidence in the agency or the APS.

Tip

Before making public comment, it is useful for employees to consider:

i. exactly what it is they intend to say or post online
ii. the language they propose to use
iii. whether the proposed comment is appropriate in the context of the employee's role, their seniority, and the work of their agency
iv. the social and political environment in which the comment is proposed to be made.

6.2.8 At all times, APS employees should be mindful of the requirements set out in regulation 2.1 of the *Public Service Regulations 1999* concerning the disclosure of information. See Section 4: *Managing information*.

Senior Executive Service

6.2.9 Senior APS employees should consider the impact of any comments they might make particularly carefully.

6.2.10 Senior Executive Service (SES) employees have a particular responsibility under section 35 of the PS Act to promote the APS Values, the Employment Principles and compliance with the Code, by personal example and other appropriate means.

6.2.11 SES employees within each agency are also part of a collective leadership group that extends across the APS. Because of the influence that they carry with stakeholders, and because they are likely to be required to advise on, or lead, the implementation of government policies and programs, SES employees should be particularly careful when making public comment. The role of SES employees provides more scope for conflict, real or apparent, between a personal view and:

a. the ability to fulfil current and potential duties in an apolitical, impartial and professional manner
b. the ability to be responsive to the Government.

Making unofficial public comment in a professional capacity

6.2.12 Some employees are subject matter experts and might seek to make comment in that capacity.

6.2.13 In such cases, it is important for the employee to notify their manager of any comment they propose to make in their 'expert' role that might reasonably reflect on their agency or their APS employment. This would need to be considered in light of the agency's policies and the APS Values, Employment Principles and the Code.

6.2.14 Agency heads and employees need to manage situations where the relationship between the employee's professional interests and their APS employment may create ambiguity about the capacity in which the employee's comments are being made. An agency head may direct the employee not to comment where necessary.

Tip

When an employee comments on a matter it can be difficult for an observer to know whether the comment is being made in a private capacity or on behalf of the employee's agency. Before making unofficial comment in such circumstances it is useful for employees to consider:

i. Is the proposed comment appropriate in the context of their duties?
ii. Can it be made clear that the comment does not represent the views of their agency or the Government?
iii. Does the comment comply with their agency's policy on making public comment in a professional capacity?
iv. Has the proposed comment been discussed with their agency?

Additional considerations when participating online

6.2.15 Maintaining an online presence, and making comment online, is a common practice in the Australian community. Like other citizens, APS employees make public comment on social networking sites, blogs, and online news sites. APS employees should comply with their agency's policies in relation to the use of work computers when participating in social media.

6.2.16 While the same principles apply to online comment as to any other kind of public comment, there are some additional considerations that apply to online participation. The speed and reach of online communication means that comments posted online are available immediately to a wide audience. Any information an employee posts relating to their employment, such as naming their employer or describing their role, can be located easily and quickly by a search engine.

6.2.17 Material published online is often difficult to erase, may be replicated endlessly, and may be sent to recipients that the author never expected would see it. Content posted by others may be perceived to be associated with material posted by an APS employee in a way that implies support for the views expressed. Failure to remove or contradict comments made on, for example, a blog or social media post may be seen as endorsement of those comments.

6.2.18 A site's security settings are not a guarantee of privacy. Material posted in a relatively secure setting can still be copied and reproduced elsewhere. Comments posted on one site can also be used on others under the terms and conditions of many social media sites.

6.2.19 APS employees must still uphold the APS Values, Employment Principles and the Code even when material is posted anonymously, or using an alias or pseudonym. Employees should bear in mind that even if they do not identify themselves online as an APS employee or an employee of their agency, they may nonetheless be recognised and identified.

6.2.20 It may also be clear that posts made anonymously have been made by existing APS employees given their content. Each such post erodes the level of confidence that the APS is serving the elected government faithfully and is committed to delivering government services.

6.2.21 As a rule of thumb, anyone who posts material online should make an assumption that at some point their identity and the nature of their employment will be revealed. When posting material, employees should be confident that, should their identity become known, the material does not raise questions about their ability to meet the behavioural standards set out in the APS Values, Employment Principles and the Code.

6.3 Providing information to parliamentary committees of inquiry and Royal Commissions in a personal capacity

6.3.1 An APS employee who makes a submission to, or appears as a witness before a parliamentary committee of inquiry or a Royal Commission should have regard to the Government Guidelines for Official Witnesses Before Parliamentary Committees and Related Matters (the Guidelines for Official Witnesses).

6.3.2 APS employee may also make submissions to a parliamentary committee of inquiry or a Royal Commission in a personal capacity. An employee appearing before a committee in a personal capacity should make it clear to the committee that their appearance is not in an official capacity. The employee must not communicate information in a way that implies their personal views are those of the agency, such as by using official letterhead or a signature block that identifies the employee's place of work. It is particularly important for senior employees to give careful consideration to the impact of any comment they might make. The Guidelines for Official Witnesses note that heads of agencies and other very senior officers need to consider carefully whether, in particular cases, it is practicable for them to claim to appear in a 'personal' rather than an 'official' capacity, particularly if they are likely to be asked to comment on matters which fall within, or impinge on, their area of responsibility.

6.3.3 Before submitting information in a personal capacity, employees should be aware of the legislation that restricts the disclosure and use of official information. See Section 4: *Managing information*. The restrictions may provide grounds for the employee not to disclose certain information.

6.4 Participating in political activities

6.4.1 APS employees may participate in political activities as part of normal community affairs. They may also join, or hold office in, political parties.

6.4.2 Public participation in political activities may raise perceptions of conflict of interest or partiality and should be considered carefully having regard to an employee's role and duties. Participation would generally not be appropriate where an employee's duties are directly concerned with advising on or directing the implementation or administration of government policy on those issues. See Section 5: *Conflict of interest*.

6.4.3 Commonwealth anti-discrimination legislation prohibits discrimination against a person on the ground of political opinion. The legislation generally permits exemptions where action that might otherwise amount to discrimination is deemed essential to meet the requirements of the job. Such an exemption applies to employees of the Australian Electoral Commission.

Wearing or displaying political material while working

6.4.4 Wearing or displaying political material by an employee is generally inappropriate. It may give the impression that the agency endorses the political material. In some circumstances, it may create doubts in the minds of clients as to whether their queries or applications will be handled impartially.

Political campaigning and fundraising

6.4.5 Some employees, as private citizens, choose to campaign for candidates for political office. The role they play may range from handing out how-to-vote cards on election day to activities with a higher profile.

6.4.6 If an APS employee has a significant role in a political campaign, there is potential for a conflict of interest between taking a position on issues and impartially performing their official duties. The employee should discuss such potential conflicts with their agency. Ways of resolving such conflicts might include the employee taking leave, rearranging existing duties, transferring to other duties, or agreeing to take a less significant role in the political campaign.

6.4.7 If an APS employee is involved in political campaigning, they should make it clear they are not undertaking these activities as part of their official duties. For example, they should not wear anything that identifies them as an APS employee at party political meetings. APS employees must not use government resources including email, telephones, photocopiers and facsimile machines for any political activity.

6.4.8 An APS employee may apply to take leave without pay, annual/recreation or long service leave to assist with an election campaign.

6.5 Standing for Parliament

6.5.1 APS employees must resign before nominating as a candidate for the Senate or House of Representatives. The election of a person who did not resign from the APS before nominating for election to the Federal Parliament would be held invalid.

6.6 Participating in state or local government activities

6.6.1 APS employees may hold an office in local government organisations. However, agency policies or practices concerning outside employment may apply, particularly if participation in local government would adversely affect the capacity of the employee to carry out their duties. It is not necessary to resign to stand for election to a local government body.

6.6.2 APS employees should take care when considering, or commenting on, political or social issues related to their local government role, to ensure it does not conflict with their official duties.

6.6.3 APS employees intending to stand for election to State Parliament, or the Northern Territory or Australian Capital Territory legislative assemblies, should seek legal advice about any legislative provisions that require them to resign from the APS.[18]

6.7 Participating in union activities

6.7.1 APS employees are generally subject to the same workplace relations arrangements as the wider community. This is recognised in section 8 of the PS Act. Employees are free to choose whether or not to be a union member. No restriction applies under the PS Act about which union they may join, or the level at which they participate in union activities.

6.7.2 APS employees taking part in union activities, for example as officers or delegates of a union, must uphold the APS Values and Employment Principles and comply with the Code, including when making public comment.

Agency policies and procedures

i. Agencies may wish to develop policies, guidance, or training to help their employees uphold the APS Values and the integrity and good reputation of their agency and the APS, including when making public comment in an unofficial capacity. For example, agencies may wish to provide guidance on:

   a. how to communicate appropriately in online forums, and how to evaluate whether a comment an employee proposes to make online is appropriate in a given set of circumstances
   b. how to avoid potential perceptions of partiality when participating in political activities
   c. appropriate use of ICT resources in the workplace, including appropriate use of work email and personal technology—such as smartphones—in work time. See Section 7: *Using Commonwealth resources*.

ii. Agencies are encouraged to ensure their managers become familiar with agency guidance on making public comment, and support them in facilitating discussions with their staff about what may be reasonable comment in a given set of circumstances. Case studies are a useful way of encouraging discussion, and the Australian Public Service Commission's REFLECT decision-making model is a helpful tool in guiding these discussions.

Making public comment and participating online

Objective

This policy provides guidance and direction to Employees of the Australian Public Service Commission ('the APSC') about the application of the APS Values and Code of Conduct to public comment that an employee may make, or is expected to make, in their official role, and to any comment they may choose to make unofficially, including online.

Application

This policy applies to all employees.

> *Note: The policy may also be extended to include contractors, being those persons employed through an employment or other labour hire agency, via the terms of the contract that governs their service. In such instances, a reference to an employee in this policy includes a reference to contractors.*

This policy should be read in conjunction with the ICT Facilities Users' policy , which describes the use of APSC information technology more broadly.

Definitions applicable to this policy

Employee – means the same as an "APS employee" as defined in the Public Service Act 1999 who is working in the APSC, and including employees on secondment to the APSC.

Public comment[1] – the term is used broadly, and includes comment made on current affairs

- at public speaking engagements
- during radio or television interviews
- on the internet (including blogs, social networking sites and other online media that allow user participation and interaction)
- in letters to the press
- in books or notices
- in academic or professional journals
- in other forums where the comment is intended for, or may be accessed by, the community.

Social Media - includes, but is not limited to online applications such as social networking sites, wikis, blogs, micro-blogs, video and audio sharing sites and message boards.

[1] From APSC Circular 2012/1

Principles

General principles

APSC employees are expected to exercise discretion and use their own judgement when making decisions about making public comment or participating online. Generally, if an employee has any doubt they are expected to seek guidance from their Manager or the Ethics Advisory Service before taking any action.

APSC employees may make public comment—including online—in a number of capacities:

- *Official*—as part of their role in the Commission
- *Unofficial*, either:
  - in a *private* capacity, or
  - in a *professional* capacity, where an employee who is also a subject matter expert makes comment on their area of expertise, but outside of their APSC role.

There are different considerations that employees need to take into account, depending on the capacity in which they are making comment.

The APSC recognises that employees have the same right of freedom of expression as other members of the community, subject to legitimate public interests such as the maintenance of an impartial and effective public service in which the community can have confidence. These public interests are protected by elements of the APS Values and Code of Conduct.

Media

Any approach to an employee by a journalist, or media or other organisation for a comment, view, opinion or policy position that may be considered to represent the Commission's position should be referred to the Group Manager, Corporate as the APSC's Media Liaison Officer before any response is made. This does not include factual material or information that is in the public domain.

General principles relating to social media

Employees are expected to consider the following information when making use of social media for work purposes, or personal use at any time, when it has or could reasonably be assumed to have a connection with the employee's employment in the APS. An obvious example is anything that is branded in connection with the APSC (including using APSC contact details and/or title) could reasonably be assumed to be connected with employment. Less obvious may be such things as identifying yourself as the author of an article published in an online journal.

Employees should consider that:

- comment made online, including in social media:
  - is available immediately to a wide audience
  - effectively endures without limit
  - may be replicated repeatedly
  - may be received by recipients it was not intended for, or who may use it for a purpose for which it was not intended, o may take it out of context, and
- a web site's security setting does not offer a guarantee that comments or dissemination is controlled, and
- even if comments are made anonymously or under an alias, and employee's identity may be revealed or inferred.

As a general principle, if an employee does identify themselves on social media as being an employee of the APSC (for example on Facebook) then it may affect employment because of the connection the employee has made between their employer and themselves.

Therefore, when make use of online media an employee must have particular regard to the following APS Values:

1. Act in accordance with the APS Code of Conduct including behaving with respect and courtesy at all times in the course of their employment
2. Deal appropriately with information, recognising that some information needs to remain confidential
3. Take reasonable steps to avoid conflicts of interest
4. Make proper use of Commonwealth resources
5. Uphold the APS Values and the integrity and good reputation of the APS at all times
6. Not act in a way that would call into question the employee's ability to be apolitical, impartial and professional in the performance of their duties.

SES employees

SES employees need to have particular regard to their activities because of their leadership role, and the real, or perceived, influence they may have with stakeholders. SES employees need to be aware that they are more likely to be perceived to be commenting on behalf of the APSC—even when making comment in a private capacity.

Making comment in an official capacity

As with any activity undertaken as an APS employee, an APSC employee making comment in an official capacity is required to act honestly, professionally, and with respect and courtesy. The APS Values stipulate that the APS is apolitical. Therefore, the role of an APSC employee in making a public comment relating to a government activity, service, or policy, via social media or otherwise, is to explain or provide information, rather than to promote or 'market' it.

Social media provides an opportunity for the APSC to engage and interact with the Australian community, seek comment or input, and provide or explain information about activities, services or policies. It allows the APSC to easily publish, share and discuss content. The APSC supports its employees' participation in social media online applications when this is a legitimate part of a business communication strategy and is a part of their official role. When doing so, an employee is required to clearly identify themselves as an APSC employee, including their role, title and contact information.

Making comment in an unofficial capacity

Employees should consider very carefully whether they identify themselves as an employee of the Commission/APS when making unofficial comment, taking into account the likelihood of being perceived to be representing the APSC.

The APSC respects the right of employees to participate in political, advocacy, and community activities. The APSC is concerned to ensure that employees conducts themselves, and are perceived as conducting themselves, in a manner that demonstrates that they can act apolitically and impartially. Therefore, an employee is expected to take reasonable steps to ensure that they do not bring into question their ability to work apolitically and impartially.

An employee must not use their official e-mail address, or other APSC livery, when making public comment that is not being made in their official capacity.

Professional

Some employees are subject matter experts in fields that may relate to their APSC employment—or which may be wholly separate from it—and might make comment in that capacity. For example, an APSC employee may publish in academic journals, or speak at professional conferences, in their own time and outside their role. In such cases, it is important for the employee to notify their Manager of any comment that they propose to make in their 'expert' role that might reasonably reflect on their employment. It is important that the employee also make it clear, when making public comment in this role, that they are not representing the APSC or the Government.

Private

APSC employees may generally make public comment in a private capacity, so long as they make it clear they are expressing their own views.

Questions or concerns

The application of the Values and Code of Conduct to a particular instance of public comment may not always be clear-cut, and that employees are encouraged to discuss these matters with their Manager, the Director, Workforce Development, or the Ethics Advisory Service.

Employees are encouraged to raise questions or concerns about the application of this policy with their manager. Managers are expected to make reasonable endeavours to resolve the matter at the local level.

Evaluation

This policy will be evaluated by the assistance it provides to employees and their manager in avoiding any real or perceived adverse issues arising from the use of social media, or other public comment.

Legislation

Public Service Act 1999

Public Service Regulations 1999

Public Service Commissioner's Directions

Consultation

Communications Team

Ethics Group

GM, Corporate (as Media Liaison)

Version control

Version no.	*Implemented by*	*Variation*	*Endorsed by*	*Review date*
1.0	*Janet Fuller*	*New policy drafted based on APSC Circular 2012/1*	*GM Corporate*	*January 2015*

Australian Public Service Commission

Information Technology (IT) Users' Policy

Revised
June 2011

Index

Section 1: Introduction 3

Section 2: Network Security 4

Section 3: Home or Remote use of IT Facilities 5

Section 4: Use of Email and Internet 5

Section 5: Monitoring use of Email, Internet and IT Facilities 7

Section 6: Protecting the Privacy of Third Parties 7

Section 7: Communications by Email 8

Section 8: On-line Participation 9

Section 9: Personal Use 10

Section 10: Failure to Comply with this Policy 13

Section 11: Reporting Suspected Breaches of this Policy 13

Section 12: Related Legislation and Policies 14

Compliance with this policy is mandated as it constitutes a lawful and reasonable direction issued by the Public Service Commissioner.

Section 1: Introduction

1.1. The Australian Public Service Commission (APSC) provides desktop access to IT facilities, including email and the Internet, to users for the purpose of carrying out the work of the APSC and assisting the Public Service Commissioner and the Merit Protection Commissioner to fulfil their statutory functions.

1.2. It is important that all users of APSC's IT facilities understand and adhere to this policy. Users include all statutory appointees, ongoing and non-ongoing employees, labour hire staff, contractors, consultants, visitors and service providers who have access to the APSC's IT facilities. The APS Code of Conduct in the *Public Service Act 1999* provides that APS employees must use Commonwealth resources in a proper manner and behave at all times in a way that upholds the APS Values and the integrity and good reputation of the APS. In addition, the Act requires 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. This policy constitutes such a direction issued by the Public Service Commissioner.

1.3. While this policy deals with your use of the APSC's IT facilities it is also important to recognise that employees engaging in on-line participation as private citizens, either on these facilities or private facilities, are still bound by the APS Code of Conduct in particular:

- to behave at all times in a way that upholds the APS Values and the integrity and good reputation of the APS; and
- to deal appropriately with information, recognising that some information needs to remain confidential.

Users are not permitted to use the APSC's IT facilities until they have acknowledged in writing that they are aware of this policy. The appropriate form is available at the end of this document.

1.4. This policy applies to the APSC's IT infrastructure and peripherals including PCs, email, Internet, Intranet, laptops, Blackberrys, desktop and mobile telephones, software and hardware such as USB storage devices. This policy also applies to the APSC's IT facilities being accessed by staff offsite, for example by those accessing the network from home.

This policy is based on the following principles:

The use of IT facilities must be consistent with the APSC's business operations and objectives.

IT resources are provided to users for work related purposes.

Reasonable personal use is permitted but must not interfere with the APSC's business operations or with work responsibilities.

Improper use of the APSC's IT facilities may lead to withdrawal of access and where considered, appropriate action may be taken under the APSC's procedures for dealing with suspected misconduct, which can lead to sanctions including termination of employment.

1.5. This policy is part of a set of documents which explains the APSC's IT facilities to staff and the associated responsibilities in relation to the use of the facilities and security of information.

These documents are:

- **Introduction to the APSC ICT environment**
  This document provides an overview of the ICT facilities. It is available on the Information Technology Intranet site.

- **IT Users' Policy**
  The document you are reading. It explains your responsibilities when using the IT equipment provided by the APSC.

- **ICT Security Policy**
  The Information and Communication Technology Security Policy addresses best practice and requirements to ensure the protection of information holdings and secure operations of APSC information and communication technology (ICT) resources.

1.6. The Department of Education, Employment and Workplace Relations (DEEWR), as our ICT service provider, has its own IT Security Policy. This document is available on the Information Technology Intranet site. The key principles of that policy and obligations that are relevant to the APSC's operations are reflected in this IT Users' Policy and the ICT Security Policy.

Section 2: Network Security

2.1. Most users will have a computer smartcard allocated to them to allow them to access the desktop computer system. Users are responsible for the safekeeping of the Smartcard. Users must not allow other people to use their smartcard.

2.2. All users have a unique password (also termed a pincode) by which the system is able to identify them. Users must not share their passwords with any other user. Users will be held accountable for misuse of IT facilities if they allow another individual to use their smartcards and/or passwords. Users must remove their smartcard when they know they are going to be away from their desks. Users are responsible for their computer if they leave it logged on and unattended for what they know will be an extended period of time. Should a user suspect that anyone has learnt one of their passwords or pincodes, the password or pincode must be changed immediately. Lost Smartcards must be reported to the IT Service Desk immediately.

2.3. Users must not engage in any activity that would compromise the security of any host computer owned by, or operated on behalf of, the APSC or the Commonwealth.

2.4. Users have a responsibility to protect the confidentiality and privacy of the APSC's data and information resources. The APSC's network is classified to store information to the level of In-Confidence. This includes Staff-in-Confidence and Commercial-in-Confidence. Material above this classification (such as Cabinet-in-Confidence) should be handled by using Secure Access Facility Environment (SAFE) which is the APSC's secure network for processing and storing of classified information up to PROTECTED level. SAFE is a secure working environment where APSC employees are able to store, edit and email PROTECTED and CABINET-IN-CONFIDENCE information. To access SAFE, contact ICT Contract Management Unit (CMU).

2.5. For further information on Network Security including advice on electronic document storage, users should refer to the ICT Security policy.

Section 3: Home or Remote use of IT Facilities

3.1. Where appropriate, the APSC has provided some users with IT facilities to use from home or other-off site locations and in some cases a remote access facility by which users can access their email accounts, files and other network services over the Internet.

3.2. The APSC's IT Users' Policy applies to IT facilities and equipment (Blackberrys, laptops etc) being used off-site in relation to:

- conduct of users while logged into the APSC network;
- documents generated or distributed while logged into the APSC network; and
- documents received from other APSC users.

3.3. At any time, the use of the APSC's IT facilities on or off-site must not be contrary to the APS Values or the Code of Conduct.

3.4. APSC staff are responsible for the security of the APSC's information and equipment when off-site. Particular care needs to be taken with classified information. See ICT Security Policy for specific information.

Section 4: Use of Email and Internet

4.1. Users of the APSC's IT facilities must not have an expectation of privacy in relation to any use they make of the system or in relation to anything they create, store, send or receive. Access controls such as passwords are designed to prevent unauthorised access and not provide privacy for the individual user.

4.2. Users should always remember that every web site they visit and email they send from APSC IT facilities can be identified and linked back to the APSC. Emails should be considered as permanent records. Furthermore, once sent they are not in the control of the sender, but the recipient. In each case, you should consider carefully how your actions could affect your reputation and that of the APSC, now and into the future.

4.3. Failure to uphold the reputation of the APS at any time can lead to misconduct action.

Section 5: Monitoring use of Email, Internet and IT Facilities

5.1. Apart from material that may be subject to intellectual property rights (for example copyright), any information/material entered or stored using the APSC's IT facilities becomes the property of the APSC. This includes all email messages users send or receive at work, even where those messages may include information or material of a personal nature.

5.2. Use of Email, Internet and all other IT access is logged. In respect of e-mails, the content, recipients and the date and time of transmission as well as other details area logged and can remain on the record even when an e-mail has been deleted. The logs may be accessed, generally by an authorised administrator and made available to authorised APSC staff for examination where there is a reasonable belief that the IT facilities have not been used in accordance with APSC IT or security policies, where a breach of the Code of Conduct is suspected, or where a subpoena or other litigation process or a Freedom of Information request requires records to be examined.

5.3. The APSC reserves the right to access any part of its IT facilities for the purposes of examining, copying or deleting any information or material stored on those facilities. The APSC retains this right as a precaution against misuse, including waste of APSC resources, fraud, workplace harassment or breaches of confidence by users.

5.4. Users will not necessarily be notified that an authorised system administrator has accessed the logs or opened an item. In some circumstances, the administrator or other authorised person may need to involve other appropriate APSC staff.

5.5. Under some circumstances, the APSC may disclose the contents of emails and logs to appropriate third parties. Examples of such circumstances include where a breach of the Code of Conduct is suspected, action in relation to a suspected criminal act is contemplated, or the information is requested through a Freedom of Information request.

5.6. Access is blocked to Internet sites that are considered unsuitable and access to which would constitute improper use. These include pornographic and violence/hate sites. The inference should not be made that where access to such sites is available that the individual user is absolved from any responsibility to exercise sound judgment.

Section 6: Protecting the Privacy of Third Parties

6.1. The Office of the Federal Privacy Commissioner recommends that clients corresponding with government agencies by email are warned that the Internet is not a secure means of transmitting information. Users in the APSC who are soliciting or sending personal information by e-mail must consider whether information being transmitted is of such a nature that directly raising the issue of the security of the Internet with the other party would be appropriate. A third party can consent to having their personal information sent over the internet but it is important that they are aware of the risks involved.

6.2. Users need to be aware of the Information Privacy Principles (IPPs) contained in the *Privacy Act 1988*. Email must not be used to disclose personal information except in accordance with the IPPs. Users should contact the Privacy Contact Officer in Legal Services for more information.

6.3. The use of portable storage devices to handle personal information also raises a number of privacy risks related to personal information storage and security. These include that personal information stored on such a device may be compromised through the operation of malicious software or the device may be lost or stolen. Such risks arise from the technical capabilities of these devices (high storage, fast speed of transfer and 'plug and play' functionality) along with their physical characteristics (small size, light weight, low cost, high portability).

6.4. Users must not use privately owned devices to connect to the APSC's network. Users are responsible for ensuring that sensitive information that is stored on portable storage devices is afforded the same protection as hard copy information. As soon as practicable, such information must be transferred to the network and deleted from the portable device. Users must report all lost or stolen portable storage devices that may store personal information to the Information Technology Security Adviser in the Corporate Group as soon as practicable after a staff member notices it is missing.

Section 7: Communications by Email

7.1. All emails sent from the APSC must be given a security classification by the user before they are sent. Mail that is not classified will not be sent to an external recipient.

7.2. Emails sent between most Commonwealth agencies are encrypted automatically using a system known as Fedlink. This means that, if an agency is on Fedlink, 'In-Confidence' material can be sent to that agency over email.[1] The list of agencies currently on Fedlink is available through the Information Technology Intranet site. Other than to Fedlink connected agencies, only emails with the classification 'unclassified or Unofficial' can be sent.

7.3. Users must comply with the *Spam Act 2003* which imposes strict controls on commercial electronic messages (CEM). IT Facilities are not to be used to conduct or

[1] Authorised users of the APSC's SAFE protected level environment may send email up to Protected classification.

advertise commercial enterprises apart from goods and services the APSC itself offers. Any e-mail promoting a training opportunity is a CEM. Emails of this nature must only be sent to those who have consented to receiving them. Consent can be express or implied in some circumstances from the relationship a user already has with the person. Emails of this nature must always contain clear identification of who is responsible for sending the email and how they can be contacted. They must also contain an unsubscribe facility allowing the addressee to opt out of receiving future messages.

7.4. Staff who receive spam must delete it immediately. Spam which could be considered distressing or offensive must not be stored on the system. Staff who receive such material very frequently and on an ongoing basis must report it to their General/Group Manager or to the Director, ICT, Corporate Group.

Section 8: On-line Participation

8.1. Risks associated with participating on-line arises from the speed and breadth of on-line communication so that one is never certain where the comment might end up or who might read it. Material posted on-line effectively lasts forever, may be replicated endlessly, and may be sent to recipients that were never expected to see the information.

8.2. All employees need to ensure that they fully understand the APS Values and Code of Conduct and how they apply to official or personal communications, including on-line communication. If in doubt, they should seek clarification from their Director or Group Manager, or consult the APSC's own Ethics Advisory Service. The APS Values and Code of Conduct apply to working with on-line media in the same way as when participating in any other public forum. The requirements include:

- 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
- at all times upholding the APS Values and the integrity and good reputation of the APS.

On-line participation in a private capacity

Employees engaging in on-line participation as private citizens on the APSC's or any other IT facilities, including private facilities, are still bound by the APS Code of Conduct, in particular:

- to behave at all times in a way that upholds the APS Values and the integrity and good reputation of the APS; and
- to deal appropriately with information, recognising that some information needs to remain confidential.

8.3. Generally, APS employees as private citizens may make public comments in a private capacity, including through on-line participation in public forums, so long as they make it clear that they are expressing their own views.

8.4. Anonymity or use of pseudonyms may not prevent you from being identified as a public servant and must not be relied upon to bypass this requirement.

8.5. APS employees acting as private citizens may not make public comments, including through on-line participation in public forums that could be perceived as:

- being on behalf of the agency or government rather than a personal view;
- compromising the APS employee's capacity to fulfill his or her duties in an unbiased manner;
- so harsh or extreme in its criticism of the government, or the alternative government(s) (including independents and smaller parties) or their respective policies that it raises questions about the APS employee's 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;
- a gratuitous personal attack; or
- compromising public confidence in the agency or the APS.

Section 9: Personal Use

9.1. The APSC allows limited personal use of its IT Facilities provided this use is in compliance with this policy and the APS Code of Conduct, is reasonable and is not improper.

9.2. A condition of any personal use is that users agree to release and indemnify the Commonwealth from and against all claims for loss or damage arising from or attributable to, their use of these systems for personal reasons/purposes. The use of these systems for such reasons/purposes will indicate the agreement of the user to providing such release and indemnity.

Limited personal use is permitted where it:

- does not interfere with the APSC's functions, operations and objectives;
- is infrequent and brief;
- does not interfere with the duties of users or their colleagues; and
- has a negligible impact on the costs and operations of the APSC.

Reasonable personal use could include:

- arranging appointments, personal travel schedule, internet banking or booking tickets on-line;
- visiting sites of personal interest including news, hobby and entertainment sites provided those sites are not improper and access is limited; and
- sending short personal messages and letters.

Improper use includes:

- distributing material, including to any personal email address, that is harmful to, or that conflicts with, the interests of the Commonwealth or the APSC;
- interfering with the authorised use of the IT facilities by others;
- use of offensive language;
- using IT facilities to harass, defame, abuse or offend;
- using the IT facilities for 'on-line' gambling;
- using the IT facilities for party political activity;
- importing, creating, intentionally accessing or attempting to access, possessing or distributing defamatory, abusive, sexist, racist, pornographic or otherwise offensive material or material likely to promote hatred or to incite violence or attempting to promote hatred or to incite violence ;
- accessing or storing any material of a sexual nature or otherwise offensive material;
- using the APSC's Internet service for streaming music or radio for entertainment purposes;

- using the APSC's Internet service for streaming audio visual for entertainment purposes;
- using the IT facilities to download large audiovisual files such as motion picture trailers, music, videos or animated cartoons;
- using the IT facilities for on-line gaming (e.g. World of Warcraft) or for participating in virtual communities e.g. Virtual Life;
- using the IT facilities to spread malicious gossip or rumours or distributing 'chain mail';
- using the IT facilities in a manner which may harm the APSC's reputation;
- using the IT facilities to make commercial gain from government information;
- using the IT facilities for private commercial activities;
- using the IT facilities to pursue private interests with colleagues, e.g. seeking signatures for private petitions, selling or advertising products/services/events;
- use of the email system to send out all staff emails on matters that are not work related;
- distributing email anonymously, using a false identity or using another person's user identification;
- using IT facilities to make public comment on political or social issues including Government policy, on behalf of the APSC which is not authorised by a Group Manager (staff are required to ensure that private comments can in no way be misconstrued as representing the views of the APSC and/or Government policy);
- any use that is not in accordance with requirements that apply to public comment and on-line participation, including as a private citizen;
- distributing communications or emails that disclose personal information without appropriate authorisation;
- any use in breach of a Commonwealth law including the Code of Conduct; and
- any use in breach of the APS Code of Conduct or APS Values.

9.3. Any attempt to bypass internet content filtering and monitoring controls is also an improper use.

9.4. Users may provide their work email address in connection with a personal transaction where doing so is not an improper use. As well as those matters described above, improper use in this context also includes circumstances where the personal transaction could be perceived as being on behalf of the APSC.

9.5. Access to social networking sites such as Facebook, Twitter and MySpace, or maintaining or contributing to a Blog or a Bulletin Board, is subject to the same requirements as all other personal use i.e. it must be limited, reasonable and not improper.

9.6. Users should seek clarification of acceptable use of IT facilities from their Director or Group Manager if they are unsure whether a proposed use is acceptable. It is the responsibility of the Group Manager to determine what constitutes unreasonable personal use, when asked for clarification by an employee.

9.7. Managers are responsible for ensuring suspected instances of misuse of IT facilities by users under their control are reported to the relevant General/Group Manager, the Group Manager of Corporate Group or the Deputy Public Service Commissioner.

9.8. Users using IT facilities are responsible for ensuring they promptly report observed instances of misuse of IT facilities to their General/Group Manager, the Group Manager of Corporate Group or the Deputy Public Service Commissioner.

Section 10: Failure to Comply with this Policy

10.1. Where there is evidence that a user has misused the IT facilities, email or the Internet, access to these facilities may be more closely monitored or suspended. In relation to employees, action may be taken under the APSC's procedures for dealing with a suspected breach of the Code of Conduct, which can lead to sanctions including termination of employment. In some cases, criminal prosecutions or other legal action may occur.

10.2. In accordance with the APSC's general approach to handling suspected breaches of the Code of Conduct, the APSC will not pay an employee's legal costs or any damages awarded against an employee as a result of unreasonable or inappropriate use. Further, if legal action is brought against the APSC, the APSC may seek to recover its legal costs and any damages payable by the APSC from the employee. In relation to other users, the relevant APSC policies and procedures will apply.

Section 11: Reporting Suspected Breaches of this Policy

11.1. All users of IT facilities should report any suspected breaches of this policy. Supervisors and managers are reminded that they must report behaviour that they suspect breaches the APS Code of Conduct by an employee for whom they have supervisory responsibility.

Section 12: Related Legislation and Policies

Archives Act 1983

Copyright Act 1968

Crimes Act 1914
Freedom of Information Act 1982
Privacy Act 1988
Public Service Act 1999

Spam Act 2003
Fair Work Act 2009

Probation and other Conditions of Engagement
Procedures for Determining Suspected Breaches of the Code of Conduct
APS Employees and Elections
Home Based Work Policy
Loss Damage and Indemnity Guidelines
Chief Executive Instruction 3: Section 6, Security of Information

Discrimination legislation and workplace relations laws may also become relevant where Internet is used improperly.

Australian Government
Australian Public Service Commission

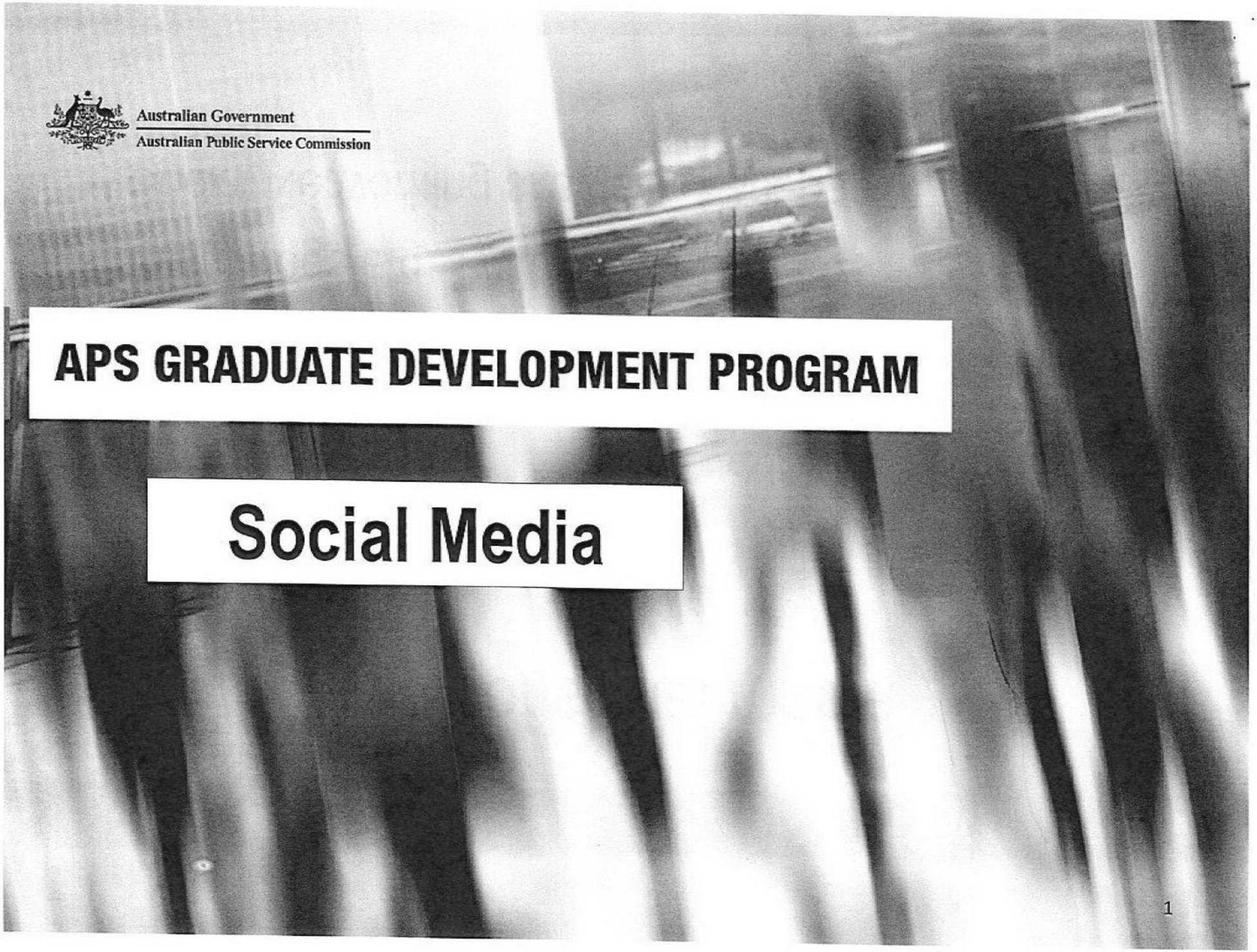
ACKNOWLEDGEMENT OF THE *IT USERS' POLICY*

The purpose of this acknowledgment is to ensure that, prior to using the APSC's IT facilities for accessing the Internet and email, staff have read and understood their obligations and responsibilities under the APSC's *IT Users' Policy*.

Section A - Employee Details	
Surname:	First Name:
Group:	Classification:
Section B – Employee Declaration	
I declare that I have read and understood the *IT Users' Policy* (as amended at June 2011) of the Australian Public Service Commission. I further declare that I understand that I am directed to comply with this policy, and that failure to comply with the direction can be a breach of s.13(5) of the APS Code of Conduct.	
Employee signature:	Date : / /
Witness signature:	Date : / /

For APS employees please return this completed form to the HR Advisor Recruitment.

For other users this form should be retained by the contract manager on the contract management file.


Australian Government
Australian Public Service Commission
APS GRADUATE DEVELOPMENT PROGRAM
Social Media

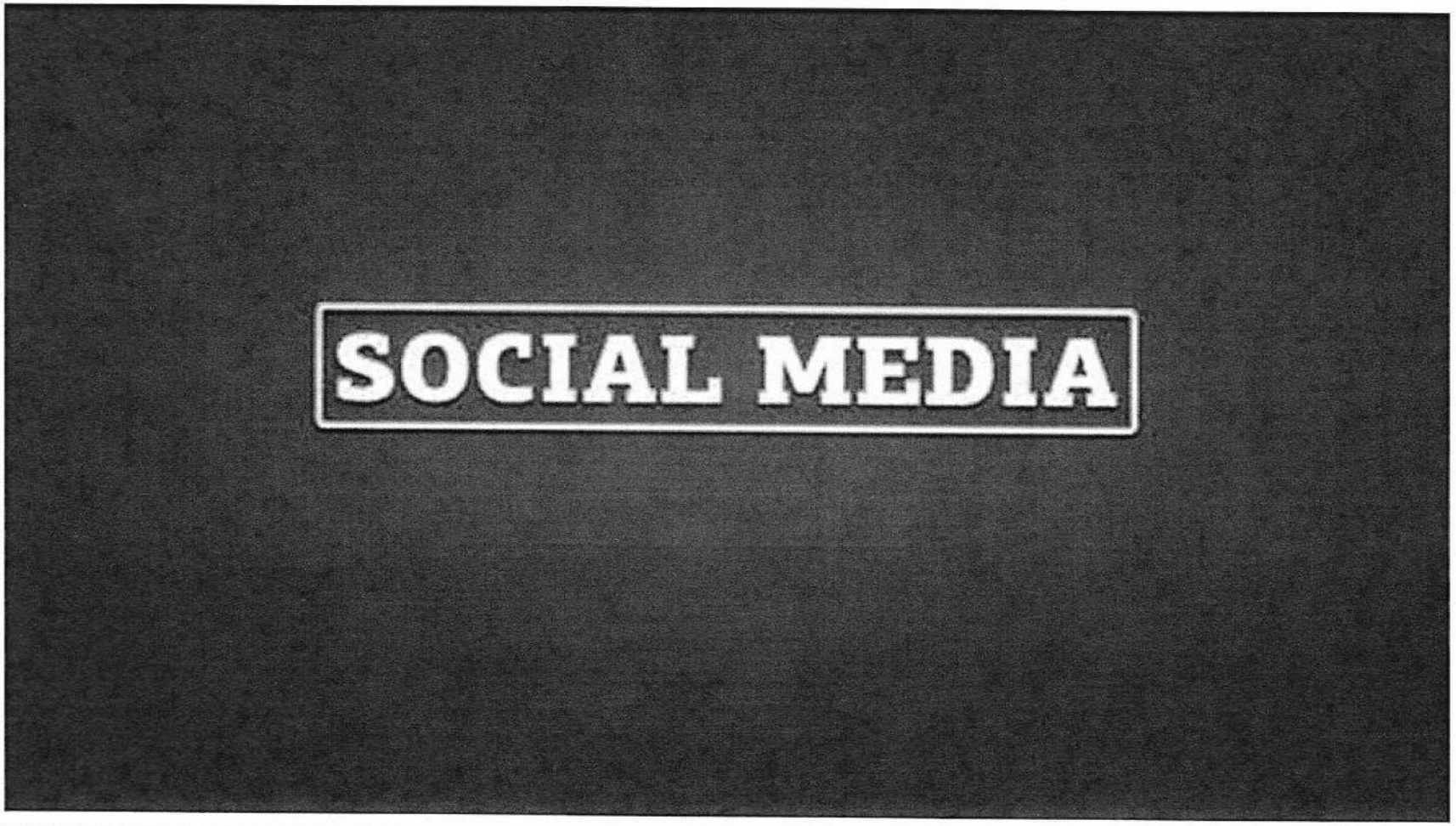
Types of social media

- Blogs
- Wikis
- Discussion forums
- Microblogs e.g. Twitter
- Social Networking sites e.g. Facebook

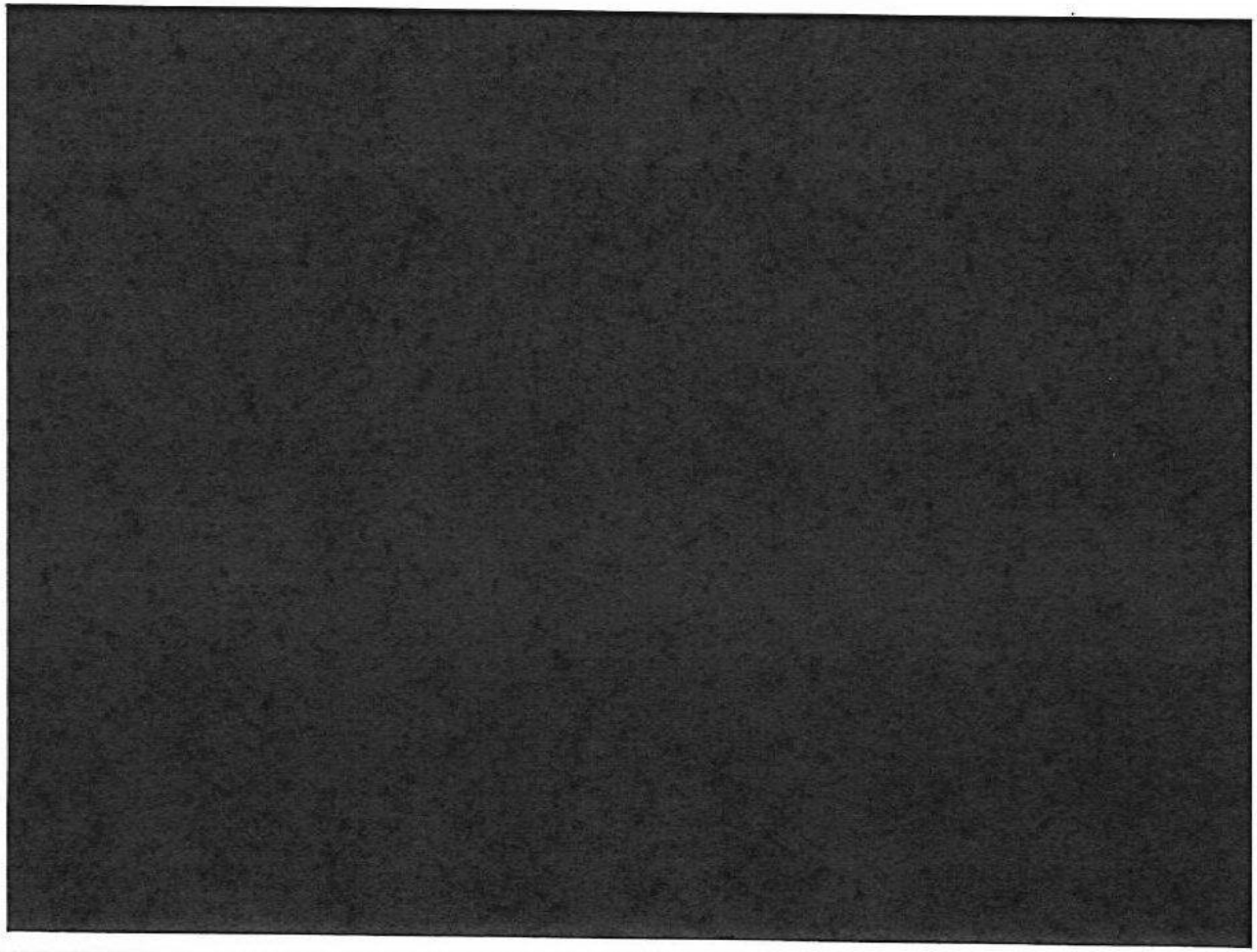
APS use of social media

- Inform the public or stakeholder groups about agency activities
- Public comment
- Collaborative document authoring
- Consultation
- Public announcements and drawing attention to new information on agency websites
- Raising public awareness of government services or initiatives
- Engaging with online communities

Social media policy



Case Study: Another Life



Inappropriate use of social media for public comment

- If it could be perceived as being on behalf of the agency or government rather than a personal view—this applies particularly to senior public servants
- If it could compromise an employee's capacity to fulfill his or her duties in an unbiased manner. This applies particularly where the comment is made about polices or programs in the employee's own agency.
- If the comment is so harsh or extreme in its criticisms of government or its policies that it raises questions about the employee's capacity to work professionally, efficiently or impartially. Such comment does not have to relate to the employee's area of work.
- If the comment is a gratuitous personal attack.
- Or if the comment compromises public confidence in the agency or the APS.

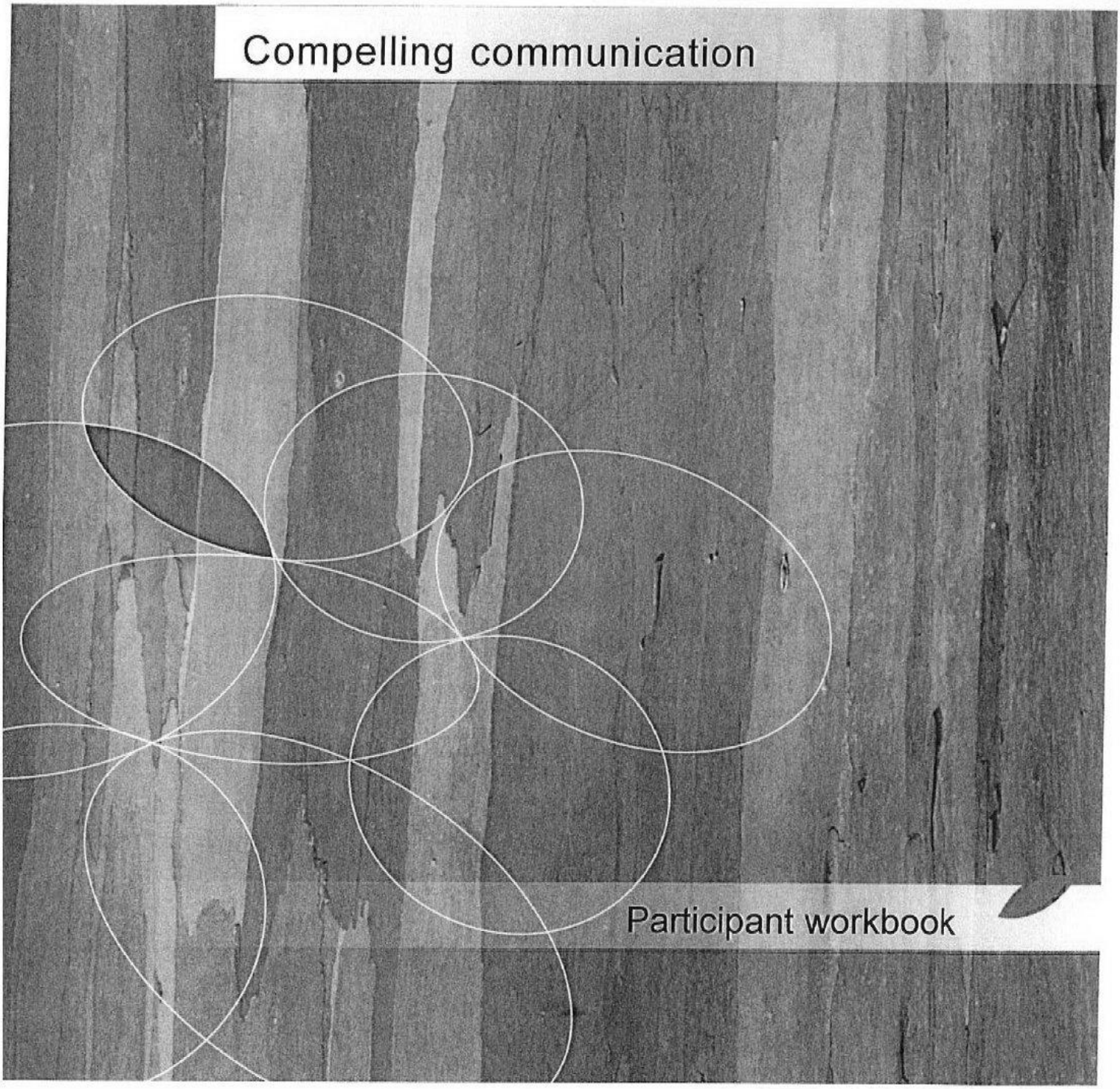
Personal action plan

- What are the main things I have learned on this program so far?
- In what areas is there room for improvement?
- What actions do I need to take when I return to work to apply and continue developing these skills?

Australian Government
Australian Public Service Commission

F1 Foundation skills

Compelling communication



Participant workbook

Effective leadership Diverse workforce ***Capable organisations and workforce*** *Employee conditions APS Values*

Unit 5: APS use of social media

Learning objectives

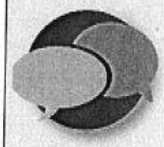
- Discuss the principles of appropriate use of social media by APS employees.

Topic 5.1 Appropriate use of social media

Social media has been identified by many areas of government as an effective medium for communicating with the public. Social media allows APS agencies the opportunity to influence, educate and engage with the community about government policies, initiatives, products and services. Social media can provide the latest, up-to-date information, while additionally allowing individuals to ask questions and receive appropriate responses.

Subsequently, many government agencies now have social media policies and guidelines. There is also the APSC's circular on making comment and participating online. To access the circular click or copy this link: **http://www.apsc.gov.au/publications-and-media/circulars-and-advices/2012/circular-20121**

Activity 5.1 APS use of social media



During Phase 1 you were asked the following questions and to bring the information to this workshop. Discuss these now as a group:

- Does your agency have a social media policy? If so, what is it?
- When using social media on behalf of your department/agency, is there a clearance process?
- What social media channels does your agency use and for what purpose?
- What risks do APS agencies face when using social media to communicate?

Click or copy this link to view the Department of Human Services Social Media Policy video: **https://www.humanservices.gov.au/corporate/media/social-media-department/social-media-policy-departmental-staff**

Notes

Notes

Activity 5.2 Another life—ethical use of social media case study

Your facilitator will show a short video of a case study of an APS employee using social media. The video can be accessed by clicking or copying this link:
http://www.apsc.gov.au/__data/assets/video_file/0006/1797/blogging.wmv

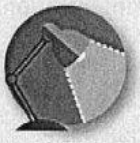
After you have watched the video, reflect on the questions below. Be prepared to discuss your answers with your colleagues.

Reflection questions—commenting publicly

- Is Will free to write anything he wants on his blog?
- How might others view Will as a result of what he has written?
- How could Will have done things differently?
- What were Tracey's responsibilities and role?
- How could Tracey have managed things better?

Reflection

Reflection



Reflecting on the exercise: Another life

Advances in technology mean there is considerable interest in the use of online communication as a means of consultation and discussion.

It is important to remember that use of online media by staff as part of their work, or in a private capacity, is governed by the same rules about using and disclosing information and making public comment that apply with other forms of communication.

Generally, public servants may make public comment in a private capacity, including on a blog, so long as they make clear they are expressing their own views. However, it is not appropriate for employees to make public comment:

- If it could be perceived as being on behalf of the agency or government rather than a personal view—this applies particularly to senior public servants
- If it could compromise an employee's capacity to fulfil his or her duties in an unbiased manner. This applies particularly where the comment is made about policies or programs in the employee's own agency.
- If the comment is so harsh or extreme in its criticisms of government or its policies that it raises questions about the employee's capacity to work professionally, efficiently or impartially. Such comment does not have to relate to the employee's area of work.
- If the comment is a gratuitous personal attack.
- If the comment compromises public confidence in the agency or the APS.

Relevant APS Values and elements of the Code of Conduct

- The APS is apolitical, performing its functions in an impartial and professional manner (s10(1)(a) of the Public Service Act).
- The APS is openly accountable for its actions within the framework of Ministerial responsibility to the government, to the parliament and the Australian public (s10(1)(c) of the Public Service Act).
- The APS has the highest ethical standards (s10(1)(d) of the Public Service Act).
- An APS employee must at all times behave in a way that upholds the APS values and the integrity and good reputation of the APS (s13(11) of the Public Service Act).
- An APS employee must comply with any other conduct requirement that is prescribed by regulations (s13(13) of the Public Service Act). Public Service Regulation 2.1 imposes a duty on an APS employee not to disclose certain information without authority (i.e. information communicated in confidence or where disclosure could be prejudicial to the effective working of government).

Tips

- Don't assume that anything done outside of working hours is not connected with work.
- Get to know how the APS values might apply outside of work. Discuss possible situations with colleagues and your supervisor.
- Find out what your agency's IT policies are, particularly regarding the use of social media.
- As a manager, explain reasons for decisions clearly—beware of making assumptions. Communicate agency IT policies well, particularly new and updated policies.