

# 08



Australian Government

Fair Work  
OMBUDSMAN

## Best Practice Guide Workplace privacy



- 01 Work & family
- 02 Consultation & cooperation in the workplace
- 03 Use of individual flexibility arrangements
- 04 A guide for young workers
- 05 An employer's guide to employing young workers
- 06 Gender pay equity
- 07 Small business & the Fair Work Act
- 08 Workplace privacy**
- 09 Managing underperformance
- 10 Effective dispute resolution
- 11 Improving workplace productivity in bargaining
- 12 Parental leave

### Working at best practice

Employers should implement best practice when it comes to maintaining privacy in the workplace. It is important for employers, employees and their representatives to know what information may be collected and retained by employers and whether it can be passed on to others. Best practice creates certainty and security for both employers and employees.

This Best Practice Guide explains:

- what is privacy

---

- what is workplace privacy

---

- general privacy principles

---

- obligations when information is provided to third parties, particularly when given under the *Fair Work Act 2009* (FW Act)

---

- privacy in relation to email and the internet.

---

There is also a checklist to assist with achieving best practice on workplace privacy.

This guide illustrates best practice when it comes to workplace privacy. For more specific information regarding your minimum legal obligations and entitlements, contact the organisations listed under the 'For more information' section at the end of this guide.

### What is privacy?

Privacy is the word we give to being able to keep certain information to ourselves and to control what happens to our personal information. It also refers to being able to do things without interference by others. Privacy issues can arise in all aspects of life.

Commonwealth privacy laws regulate the collection and handling of personal information through minimum privacy standards. These are known as the Australian Privacy Principles (APPs). The APPs apply to all private sector businesses with an annual turnover of more than \$3 million, all private health service providers nationally, a limited range of small businesses and all Australian government agencies. Although some small businesses are not required to abide by Commonwealth privacy laws, all businesses should aim to comply with the privacy principles as a matter of best practice.

For specific information about APPs visit the website of the Office of the Australian Information Commissioner at [www.oaic.gov.au](http://www.oaic.gov.au).

### What is personal information?

Personal information is information that identifies a person. There are some obvious examples of personal information such as a person's name or address. Personal information can also include photos, credit history information, bank account details and even information about what a person likes, their opinions and where they work - basically any information where the person is reasonably identifiable.

Personal information can be sensitive in nature such as information about a person's race, ethnicity, political opinions, membership of political associations, membership of professional associations and trade unions, religious or philosophical beliefs, sexual preferences, health and genetic information or criminal records. The APPs provide higher privacy standards when organisations are handling an individual's sensitive information. Best practice employers apply the same higher standards even where they are not covered by the *Privacy Act 1988* (Cth) to ensure that sensitive personal information is handled appropriately.

### What is workplace privacy?

Employers will have access to personal information about employees. This information may be sensitive and employees may wish to keep this information private. This means that employers will need to think about the way in which they collect, use and disclose information they obtain from employees.

In many cases, Commonwealth privacy laws will not apply when it comes to employee records. Commonwealth privacy laws only apply to employee personal information if the information is used for something that is not *directly* related to the employment relationship between the employer and the employee. Nonetheless, best practice employers think carefully about any personal information that they have about their employees and treat that information in accordance with the privacy standards set out in the APPs.

It is good privacy practice for employers to tell employees when they collect their personal information. In doing so, the employer could tell the employee why they are collecting the information and who the employer might pass that information on to.

Best practice employers allow employees to access personal information about themselves which is held by their employer. Employees should also be able to have that information corrected or verified if it is incorrect, out of date or incomplete.

### General privacy principles

The Office of the Australian Information Privacy Commissioner's website contains further information on good practice for organisations dealing with employees' personal information. The guides deal with:

- limiting the collection of information

---

- providing notice to individuals about the potential collection, use and disclosure of personal information

---

- disclosing personal information

---

- keeping personal information accurate, complete and up-to-date

---

- keeping personal information secure

---

- providing access to personal information.

## When can you give information to third parties?

Best practice employers understand that creating trusting relationships with employees is integral to achieving a happy and productive workplace. Best practice employers follow the APPs when providing information about their employees to third parties. In line with the APPs, for example, an employer should not sell a list of its employees to another organisation for marketing purposes.

In limited circumstances, however, an employer may disclose employee records to a third party.

### Information requested by a Fair Work Inspector

A Fair Work Inspector can request information about employees in order to establish that the business is meeting its employment obligations. Under the FW Act, employers are required to provide this information to a Fair Work Inspector.

### Information requested by other government agencies

Some government agencies, such as the Australian Tax Office, have powers to request information from employers. Employers should satisfy themselves that the agency requesting the information has the power to do so. You may wish to ask the agency what law allows them to make a request for the information. When required by law, employers should provide the requested information to the appropriate government agencies.

### Information requested by a permit holder

There may be occasions where a permit holder (generally a union official) will wish to enter an employer's premises to investigate a suspected contravention of the FW Act or an industrial instrument such as a modern award or enterprise agreement. While on the premises, the permit holder may also ask to inspect or copy documents.

In these circumstances, the FW Act:

- allows a permit holder to inspect or copy documents which are directly relevant to the suspected contravention

---

- allows a permit holder to inspect or copy the documents of members of the organisation the permit holder is from

---

- allows a permit holder to inspect or copy the documents of non-members where consent has been obtained from the specific non-members or an order for access has been obtained from the Fair Work Commission

---

- exempts an employer from allowing the permit holder to inspect or copy documents if doing so would contravene a Commonwealth law (including the Commonwealth privacy laws) or a state or territory law.

---

The FW Act also imposes certain privacy obligations on a permit holder (and the organisation they are from) in relation to information obtained from the exercise of a right of entry. Subject to limited exceptions, a permit holder and the organisation must not use or disclose personal information obtained in these circumstances for a purpose other than to investigate or remedy a suspected contravention.

A permit holder or organisation found to have breached these obligations can be liable for significant penalties and may have their permit revoked.

Information collected from a protected action ballot  
Protected action ballots will generally be conducted by the Australian Electoral Commission (AEC). Under the FW Act, however, the Fair Work Commission may decide that a person other than the AEC is to be the protected action ballot agent or independent adviser for a protected action ballot.

In this situation, the non-AEC ballot agent or independent adviser must not disclose information that would identify an employee as a member or non-member of a union. Disclosure of such information may be subject to a civil penalty under the FW Act. It may also be the subject of the Commonwealth privacy laws and a complaint to the Office of the Australian Information Commissioner.

### Information for references

Sometimes employers are approached to provide employment references about former or current employees. Providing information that relates directly to the employment relationship between an employer and employee is not a breach of Commonwealth privacy laws. Information that directly relates to the employment relationship can include things such as the employee's skills, performance, conduct, and their terms of employment.

In general, best practice employers consider whether to disclose personal information about an employee without their consent. If an individual applying for a job has asked a former employer to act as a referee, the former employer can assume, when contacted for a reference, that they have the individual's implied consent to disclose relevant information about them. However, if the former employer has not been asked by the individual to be a referee and is contacted for a reference, generally the former employer should seek the consent of the individual before disclosing information about them.

Best practice employers also consider what information is appropriate to provide in a reference. In some circumstances, it may not be good practice to disclose personal information about, for example, an employee's medical history. The Office of the Australian Information Commissioner can provide more information on this matter.

### What about email and the internet?

Employee and employer use of internet and email can raise issues about workplace privacy. Password access and login codes may give employees the impression that their email and web browsing activities during work hours are private. Employees may not be aware that these activities can be scrutinised by their employer.

Clear workplace policies can help to ensure that both employees and employers understand the expectations and responsibilities that apply to email and internet use.

The preparation of a best practice internet and email usage policy can include:

- consulting with employees about the policy during the policy's development. This will help the employer to understand the types of legitimate activities for which staff are using email and web browsing. A consultative process can also increase employees' awareness of the possible risks to the business associated with improper email and internet use

---

- developing and communicating to the employees a policy which outlines the obligations and responsibilities of employees and the employer in relation to use of electronic communication mediums. A best practice policy will:
  - explain clearly what is appropriate use of email and internet at work
  - outline what personal use of email both within the organisation and externally, is appropriate
  - outline types of use that are prohibited
  - refer to any relevant legislation regarding use and access
  - outline what information is logged and who in the organisation has rights to access the logs and content of staff email and browsing activities
  - set out in plain English how the business intends to monitor or audit employee compliance with its rules relating to acceptable usage of email and web browsing
  - outline potential consequences for misuse of email or web browsing.

---

- reviewing the policy with employees on a regular basis. This will help the policy to keep up with the development of the internet and information technology. The policy should be re-issued to all employees whenever significant change is made so they are aware of any change and to reinforce the organisational message.

Similar issues (and best practice responses) may arise from the use of company-provided mobile phones and other electronic devices when accessed for personal use.

### What about other legal requirements?

Some states and territories have their own laws that may relate to workplace privacy or workplace surveillance. See the 'For more information' section at the end of this guide to find out where to learn more.

### Checklist for best practice on workplace privacy

- ✓ Is there a policy and practice on how employee personal information is collected and handled?

---
- ✓ If so, how is the policy and practice communicated to staff and how are people made aware of it? How is it made available to employees?

---
- ✓ Does the business only collect and retain information about employees that is necessary?

---
- ✓ Is personal information held by the business complete and up-to-date?

---
- ✓ Does the business retain personal information in a secure way?

---
- ✓ When providing information to a third party, has the business ensured that it has complied with its own privacy obligations? For example, if information is being provided to meet a lawful request, has the business only provided information that is necessary to comply with that request?

---
- ✓ Does the business have policies in place about use of electronic equipment which sets out appropriate personal and business use and which makes clear how the business monitors employee use of electronic equipment?

---

## For more information

### Office of the Australian Information Commissioner (Oaic)

1300 363 992  
[www.oaic.gov.au](http://www.oaic.gov.au)

To find information about  
privacy laws in your state, visit:  
[www.oaic.gov.au/privacy/  
privacy-in-your-state/](http://www.oaic.gov.au/privacy/privacy-in-your-state/)

### Fair Work Ombudsman

13 13 94  
[www.fairwork.gov.au](http://www.fairwork.gov.au)

### Fair Work Commission

1300 799 675  
[www.fwc.gov.au](http://www.fwc.gov.au)

## Acronyms used in this guide

**AEC** Australian Electoral Commission

---

**FW Act** *Fair Work Act 2009*

---

**APP** Australian Privacy Principles

---

## Disclaimer

The Fair Work Ombudsman is committed to providing you with advice that you can rely on.

The information contained in this Best Practice Guide is general in nature. If you are unsure about how it applies to your situation you can call our Infoline on 13 13 94 or speak with a union, industry association or a workplace relations professional.

Updated October 2019. FWOBPG8a.03.

© Commonwealth of Australia 2019



Australian Government

**Fair Work**  
OMBUDSMAN

Fair Work Ombudsman  
13 13 94  
[www.fairwork.gov.au](http://www.fairwork.gov.au)