Australian Government

Fair Work OMBUDSMAN

Workplace privacy best practice guide

Australian Government Fair Work OMBUDSMAN

Workplace privacy best practice guide

This best practice guide is for employers and managers. It explains the Australian Privacy Principles and your obligations when managing employees' personal information.

It includes:

It also has practical tips and case studies to help you move your business towards best practice.

Working at best practice

Best practice employers know how important it is to keep their employees' personal information private. They have clear policies that set out exactly what information the business can collect and keep, and when it can be passed on to others.

Every workplace can enjoy the benefits of taking a best practice approach to workplace privacy. These may include:

- complying with legal obligations
- increased employee confidence and trust
- certainty and security for both you and your employees.

Privacy and personal information

Privacy is our ability to protect our personal information including being able to control who can see or use information about us.

Personal information is information that says who we are, what we do and what we believe. Names, addresses, phone numbers, email addresses, photos, bank account details, tax file numbers, super fund information, drivers licence details and academic records are a few examples.

Personal information can be sensitive in nature, for example, information about a person's health, sexuality, religious beliefs, criminal record, professional or trade union memberships. This kind of personal information is known as sensitive personal information.

Legal requirements

Australian Privacy Principles

The Privacy Act 1988 sets out requirements for collecting, storing, using and disclosing personal information. These are called the Australian Privacy Principles. The *Privacy Act 1988* also sets out additional rules and higher standards for collecting and handling sensitive personal information.

They apply to:

- businesses with an annual turnover of $3 million or more
- all private health service providers
- a limited range of small businesses
- all Australian Government agencies.

If you're required to follow the Australian Privacy Principles, you must have a privacy policy. For more information, refer to the Office of the Australian Information Commissioner's website at oaic.gov.au

All businesses should aim to comply with the privacy principles as a matter of best practice. However, not all businesses are subject to Commonwealth privacy laws.

Rules about employee's personal information

The Fair Work Act requires all employers to keep certain personal information about employees in their employee records.

Personal information held by an employer, relating to someone's current or former employment, isn't covered by the Australian Privacy Principles, but only when used by the employer directly in relation to their employment. This information includes:

- the employee's personal and emergency contact details
- information about terms and conditions of employment
- wage or salary details
- leave balances
- records of work hours
- records of engagement, resignation or termination of employment
- information about training, performance and conduct
- taxation, banking or superannuation details
- union, professional or trade association membership information.

The Australian Privacy Principles do apply to personal information about unsuccessful job candidates. This can include applicants' resumes, contact details, references and academic transcripts.

Third parties providing recruitment, training, human resources, payroll or other services to the employer under a contract may need to comply with the Australian Privacy Principles.

Disclosing pay and workplace conditions

Under the Fair Work Act, employees have workplace rights to share or not share information about:

- their pay
- their employment terms and conditions that would be needed to work out their pay, such as their hours of work.

They also have the right to ask other employees (with the same or a different employer) about:

- their pay
- their employment terms and conditions that would be needed to work out their pay, such as their hours of work.

Employees can't be forced to give this information to another employee if they don't want to.

Employers can't take adverse action against an existing or future employee either:

- because of these rights or
- to prevent an existing or future employee from exercising these rights.

For more information about these rights, including when these rights started applying and who they apply to, see Prohibiting pay secrecy at fairwork.gov.au/pay-secrecy

Disclosing employee personal information to third parties

You can legally disclose employee records to a third party in some circumstances, for example as detailed below. Employees are also entitled to access to their own employment records.

Information requested by a Fair Work Inspector

A Fair Work Inspector can request information about employees to check your business is meeting its employment obligations. Employers are legally required to provide requested employment records to a Fair Work Inspector in some circumstances, for example if they issue a 'notice to produce' that requires records or documents to be produced.

For further information about the powers of Fair Work Inspectors see our Record-keeping and pay slips online course at fairwork.gov.au/learning

Information requested by other government agencies or by law

Certain government agencies (such as the Australian Taxation Office, National Disability Insurance Agency and Services Australia) may ask you to provide personal information about your employees. Also, you may need to provide information to police or under court orders.

If you receive such a request, ask the person making the request which law requires or allows you to disclose the information.

Information requested by a permit holder

There may be times when a permit holder with a right of entry permit (usually a union official) wants to enter your workplace to investigate a suspected breach of workplace laws. While there, they may ask to do things like inspect or copy documents or interview people.

Permit holders can inspect and copy any record or document that's directly relevant to the suspected breach if that record or document is kept on the premises or accessible from a computer kept on the premises. They can also give written notice requiring you to produce, or provide access to, records or documents later.

The records must substantially or entirely relate to a member of the union unless the Fair Work Commission allows otherwise.

You don't need to let the permit holder inspect and copy documents if doing so would contravene a Commonwealth law (including Commonwealth privacy laws) or a State or Territory law.

See our webpage on The role of unions at fairwork.gov.au/unions for more information, including entry permit requirements and giving notice of entering a workplace.

Information requested by an employee or former employee

If an employee or former employee requests access to their own employment records you must make a legible copy available for them to inspect and copy.

If the employee record is kept at the workplace, you must make the copy available there within 3 business days or post a copy to the employee within 14 days after receiving the request.

If the employee record is not kept at the workplace, you must make a copy available or post it to the employee as soon as practicable.

Providing references

You may be approached to provide employment references about former or current employees.

You won't breach Commonwealth privacy laws if you provide personal information that relates directly to the employee's employment, but you can still ask for their consent. This can usually be assumed if they have already asked you to be a referee. If they haven't, you should consider seeking their consent before disclosing information about them.

Consider what information is appropriate to provide in a reference. Keep your comments focused on the employment relationship to avoid any possible privacy issues. This includes the employee's skills, performance, conduct, their type of employment and length of employment.

It is generally not appropriate to disclose private information about a current or former employee (for example, their medical history). As mentioned, Commonwealth privacy laws set a higher standard for collecting and handling sensitive personal information.

PRACTICAL TIP: Create a policy on employment references.

This could include in what circumstances references will or won't be given, the form of reference (written or verbal), the process for requesting a reference and a consent form.

Some employers have a policy of not providing references, and only confirming whether the employee worked for their organisation. If you adopt this policy tell the reference checker that it is a general policy and not a reflection on the specific employee.

Using best practice to protect personal information

Best practice doesn't look the same for all employers. The way to achieve best practice will vary depending on the industry, number of employees, and the business environment.

Below are initiatives and suggestions that can help you move your business towards best practice.

Commit to the privacy principles

Best practice employers choose to meet the requirements of the Australian Privacy Principles even if they aren't required to. They also apply the principles to employee records although this isn't required by law.

Tell employees what happens to their personal information

Best practice employers tell employees:

- what personal information they collect
- why they are doing so
- who they might pass that information on to
- how they can access their own personal information
- how to verify or correct their personal information if it is incorrect, out of date or incomplete, even when not required to by law.

You can include this information in your induction training, a workplace privacy policy and other staff communications.

Set clear expectations about electronic communications, social media and use of monitoring technologies

The use of internet, email, social media and employer-supplied devices (such as smart phones and tablets) affects many aspects of our working lives, including privacy.

Best practice employers have clear workplace policies to help employees understand the expectations that apply to social media, email, internet use and the use of surveillance or other data collection technologies in their workplace.

The key points to communicate to your staff are:

- electronic communications and social media aren't private
- the business can delete data and information employees have put into its systems at any time
- what is and isn't acceptable use for email, social media and internet at work
- not to disclose personal information about customers or colleagues (including images of them) through social media, email or other mediums
- the business monitors compliance with its privacy, social media and acceptable usage policies, and the possible consequences of breaching these policies
- what information is recorded and kept by the business (such as content and patterns of employees' emails and browsing activities, or location information) and who can access these records

- what, if any, areas are under surveillance (including CCTV and drones) and who has access to the information (State and Territory laws may limit when surveillance can be conducted in the workplace and elsewhere. See Links and resources for links to information in your State or Territory).

Businesses are increasingly using technology (such as apps, monitoring software or tracking devices) to supervise their employees. This may include monitoring:

- an employee's work output
- how employees are using business property (for example, when employees use their employer's property to work from home)
- employee attendance at work (for example, to satisfy workplace health and safety requirements).

There may be privacy implications when employers use technology to monitor the behaviour of their employees. For more information on surveillance and monitoring laws, refer to your State or Territory privacy body.

Develop a workplace privacy policy

Developing a workplace privacy policy can help you apply good privacy practices in your workplace.

Having a clear policy helps you ensure a consistent approach to workplace privacy. It also lets your workforce know that you take protecting their personal information seriously.

Your policy should:

- state what personal information your business collects about your employees and why
- contain guidelines limiting the collection of personal information, so that information is only collected if it's necessary for your business functions or activities or required by law
- tell employees about the processes for accessing and correcting personal information
- detail how you will respond to requests for personal information from third parties. Key considerations include:
    - who is requesting the information
    - whether the information is being provided to meet a lawful request
    - whether the information is necessary to comply with the request
- state how you will respond to requests for references, including:
    - what information will be provided (such as start and finish dates, job title, key responsibilities)
    - who'll handle reference requests
    - who can authorise references on the employer's behalf
- detail how you will deal with job applications from unsuccessful candidates. This could include:
    - a procedure for handling documents during the recruitment process, such as keeping paper and electronic copies locked away and only accessible to people with a genuine need to access them

  - specifying a timeframe for the destruction of all paper and electronic copies of recruitment materials
  - requiring the person in charge of the recruitment process to ensure all copies are destroyed
  - a procedure for responding to requests from unsuccessful candidates, including who'll be responsible for responding to the candidate
- contain guidelines for the use of electronic communications and social media
- note any monitoring, data collection or surveillance technology used in the workplace, and detail how the information will be used and stored, as well as who can access it
- tell employees about the possible consequences of the unauthorised disclosure of personal information.

The Australian Privacy Principles may require you to have a clear and up-to-date privacy policy, detailing the kinds of personal information your company holds, how you collect and store that information, and the purposes you can use the information for, as well as about accessing stored information, whether information is likely to be sent overseas, and how to complain about breaches of privacy.

CASE STUDY – Requests for employee information

Helen owns a wholesale business. People call the general number sometimes asking for information about employees. Helen included a procedure in the workplace privacy policy that requires these requests to come to her.

This process lets Helen find out what information is being requested and why. It also allows Helen to discuss the request with the employee concerned.

PRACTICAL TIP: It's essential you regularly review and update your privacy policy. This is especially important in workplaces where there are rapid developments or changes in the way employees, managers and business owners are using technology, which can have implications for the protection of personal information.

Make sure you consult with employees and managers about what they think is working and what could be improved when it's time to review your policy.

Help your managers and employees understand workplace privacy

Best practice employers give their managers and employees training about workplace privacy. This builds confidence in understanding how personal information is handled within the workplace. It could also encourage employees to keep their information up to date and discuss any issues with you or their managers.

Consider providing information and resources to reinforce your training. This could include:

- copies of policies dealing with workplace privacy
- checklists to show what information needs to be recorded and when
- guidance about the use of electronic communications including social media
- links to external resources, such as the Office of the Australian Information Commissioner at oaic.gov.au

CASE STUDY – Employee accountability

Marco is the Human Resources Manager in a professional services business. Marco explains to employees that the business will take disciplinary action for repeated breaches of its privacy and electronic communications policies. He does this during the induction of new employees and when training managers.

Marco believes these reminders help drive home the responsibilities of employees and the importance of protecting the privacy of personal information. It also makes sure staff know they're accountable if they don't comply.

Best practice checklist

A best practice workplace involves more than just understanding and complying with the law. This checklist will help you work towards best practice when managing and protecting your employees' personal information:

- ☐ **develop a policy** – develop a workplace privacy policy to explain the collection and handling of employee personal information, and find out if this is a legal requirement for your business under the Australian Privacy Principles.
- ☐ **secure personal information** – keep employee personal information secure.
- ☐ **third parties** – consider your privacy obligations when providing information to third parties.
- ☐ **electronic and social media** – develop policies to support the use of electronic communication and social media within the workplace. This will help you explain what is appropriate personal and business use, as well as how the business intends to track usage.
- ☐ **training** – provide training and resources to managers. This can assist with ensuring managers only collect and retain information about employees that is necessary.
- ☐ **communication** – communicate with your staff about privacy issues. This will help ensure that employees are aware of the policy and understand how their personal information will be treated.

Links and resources

Resources

- The Office of the Australian Information Commissioner's webpage provides a number of resources on the meaning and application of privacy law in Australia. Visit oaic.gov.au/privacy-law
- You can also subscribe to their eNews for updates and information. Visit oaic.gov.au/updates/sign-up

Links

Fair Work Ombudsman

fairwork.gov.au

State & Territory bodies

- ACT Human Rights Commission
  hrc.act.gov.au
- Information and Privacy Commission New South Wales
  ipc.nsw.gov.au
- Office of the Information Commissioner Northern Territory
  infocomm.nt.gov.au
- Office of the Information Commissioner Queensland
  oic.qld.gov.au
- Privacy Committee of South Australia
  archives.sa.gov.au/privacy-committee
- Ombudsman Tasmania
  ombudsman.tas.gov.au
- Office of the Victorian Information Commissioner
  ovic.vic.gov.au
- Office of the Information Commissioner Western Australia
  oic.wa.gov.au

CONTACT US

Fair Work online: fairwork.gov.au

Fair Work Infoline: **13 13 94**

Need language help?

Contact the Translating and Interpreting Service (TIS) on **13 14 50**

Help for people who are deaf or have hearing or speech difficulties

You can contact us through the National Relay Service (NRS).

Select your preferred access option and give our phone number: **13 13 94**

Last updated: October 2024