Click the black arrow to the right to toggle Title and border

Social media, privacy and the workplace

# Frequently asked questions from employers

## How can organisations respond when an employee has misused social media in their personal life, or in the course of their work?

If there is a legitimate purpose for collecting personal information from an employee’s social media account, organisations may be able to do this consistently with IPP 1.1. Privacy law is unlikely to stand in the way of the collection of personal information for investigatory purposes if an employee has misused social media – for example, if they have made inappropriate public comments regarding their organisation, or are involved in bullying, harassment, defamation, or other criminal activity.

Collection of personal information in the context of an investigation into social media misuse still requires organisations to consider what is reasonable under the collection principle (IPP 1).

Organisations should still only collect information by lawful and fair means, and not in an unreasonably intrusive way (IPP 1.2) and should consider whether it is reasonable to provide a notice of collection to the employee(s) involved in the incident (IPP 1.3).

Employee personal information that has been collected from social media platforms should continue to be handled in accordance with the rest of the IPPs.

**More information:** View [OVIC’s Guiding Principles for Surveillance](https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance/) and supporting [Case Studies on using a communication platform to monitor employees](https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance/)

## Is there a privacy risk in accessing or monitoring employees’ personal social media accounts?

Merely seeing personal information on social media would not necessarily constitute a collection under IPP 1. However, if this information is used for any purpose – such as to inform a human resource decision or to undertake disciplinary action – it would be considered to be ‘collected’ and must be handled according to the IPPs. Informally ‘checking up’ on employees via their personal social media accounts may be problematic as it can be difficult for employers to define precisely when information discovered on social media informs decisions made in the workplace.

It is unlikely that organisations would have a legitimate need to actively monitor its employees’ personal use of social media. However, if an organisation believes that it is necessary for its functions to regularly or intermittently monitor employees’ use of social media, it should take steps to notify its employees of this practice, such as including information in a social media policy or induction pack. Clear, up-front communication between employers and employees about any monitoring practices being used, and for what purposes, can help mitigate the risk of a privacy breach, as well as help prevent an erosion of trust between employee and employer.

While it may not violate the IPPs for an organisation to access the personal information of an employee through social media, it may give rise to other legal risks. Individuals’ social media accounts often contain a large amount of sensitive or delicate information about their private lives, much of which is unlikely to have any bearing on their work performance. Once that information is collected, organisations may be exposed to claims that adverse management or other decisions were made on improper grounds.

If an organisation chooses to monitor employees’ use of social media, they should document these activities. Most social media sites are dynamic environments, where permissions to view certain content can be easily changed, and posts and user accounts can be edited or even deleted. Organisations may have difficulty relying on information sourced from social media unless they have detailed records of when the information was collected, how it was accessed, and the permissions attached to the information at the time. This is important for ensuring the quality of data, under IPP 3.

## What can organisations do to support employees using social media?

Having a clear social media policy can help mitigate many potential issues regarding the privacy of individual employees. A social media policy should include recommendations on what is considered inappropriate for an employee to post on their personal social media accounts, and any instances where the organisation may seek access to employees’ personal information via social media.

Further, organisations need to be aware of the risks that social media may pose to their employees’ privacy as individuals through the course of their work. For instance, in some circumstances social media can provide an avenue for members of the public to identify employees of organisations. Employers with frontline staff should ensure that they are aware of the possibility that aggravated clients could search for them online, and provide support to any employee who may be subject to online harassment.

# Frequently asked questions from employees

## Is the personal information I post online protected by the PDP Act?

The PDP Act does not apply to information that is contained in a ‘generally available publication’. Intuitively, this suggests that any information that is published online and available to anyone is therefore not covered by the PDP Act. However, this may not always be the case.

In 2016, the decision of the Supreme Court of Victoria in *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 (11 October 2016), [83]–[84] (Bell J) noted that just because information might be accessible somewhere on the internet, it does not necessarily mean that the information is a ‘generally available publication’ to which the PDP Act and the IPPs do not apply.

Whether publicly available information amounts to a ‘generally available publication’ will depend on a range of factors such as the nature of the information, its prominence, the likelihood that it will be accessed, and the steps needed to obtain that access.

Despite the Supreme Court decision, the PDP Act does not necessarily prevent an organisation from collecting personal information where authorised by the IPPs. If there is a cause for collection of personal information that is covered by the PDP Act, the organisation will be able to do so regardless of whether it is on a social media platform or not.

In practice, this means that people need to be aware that when publishing content on a personal social media account (even with heightened privacy and security settings), privacy law is unlikely to stand in the way of personal information being collected and used if there is a legitimate purpose for doing so.

Regardless of the source from which personal information is obtained, if it is collected by an organisation that is subject to the PDP Act, that information should be used, disclosed, and protected according to the IPPs.

The PDP Act does not cover individuals acting in a personal capacity. This means that a privacy right cannot be enforced against an individual. For example, if an individual acting in a personal capacity posts personal information online about another individual without their consent, it is unlikely to be covered by the PDP Act. However, there may be other courses of action that could be taken against them under copyright or defamation law.

**Remember:** Personal information shared online may be permanently recorded and individuals may not be able to control the spread of that information, including who accesses, records, and uses it, and for what purpose.

## How can I manage the relationship between my professional and personal life with regards to social media?

As social media continues to blur the distinction between professional and personal life, employees may feel the need to manage their online profiles based on the knowledge that different audiences (employers, friends or family) may have access to that content. The idea that individuals constantly manage their identities based on the context they are in is not new, however social media can sometimes challenge this process.

While we may feel we have the right to conduct ourselves in any way we like on our personal social media accounts, the Victorian Supreme Court case of *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 (11 October 2016), [83]–[84] (Bell J) demonstrated that privacy law will not stand in the way of this information being collected and used if there is a legitimate purpose for doing so. Instances of bullying, harassment and defamation may warrant an investigation, which may include the collection of personal information regardless of whether it from a personal or professional account.

It is important for employees to be aware of what is and is not considered appropriate for them to post on their personal social media accounts. If an organisation does not have a specific social media policy, employees should consider asking for clear guidance on this. If in doubt, the Victorian Public Sector Code of Conduct provides broad guidelines on this topic.

## I am my organisation’s social media administrator. What are the key privacy considerations I need to keep in mind?

Consider the devices that will be used for any official social media accounts. For example, if an employee uses their personal smartphone to monitor and post to Twitter, this creates an increased privacy risk for both the employee’s own personal information as well as the organisation’s information.

No matter how technologically savvy a social media administrator may be, there is always a risk of human error. Having an official social media account attached to a personal device can increase the risk of accidentally publishing personal or sensitive information. Further, in the event of a privacy or security breach, it is likely that the employee will be required to hand over their device for investigatory purposes. Limiting social media use to work devices is therefore a good way of protecting an employee’s own personal information.

It is also important to ensure that only those employees who are authorised or properly trained for social media use have access to the accounts. Keeping passwords secure and logging out of accounts will help to mitigate the risk of unauthorised access to or disclosure of information.

## I believe my employer has been monitoring my activity on social media. What can I do?

The first thing to do is to check your organisation’s policies regarding social media and employee monitoring or surveillance. If this information cannot be found, or if your organisation does not have a clear policy regarding these practices, it is worth making enquiries about your rights and responsibilities with your organisations’ HR representative.

As noted above, ‘monitoring’ may not necessarily involve the collection of personal information under IPP 1. Generally, personal information is only considered to have been ‘collected’ if it is used by an organisation for any purpose, such as to inform workplace decisions. Collecting information from employees’ social media accounts that is not necessary for an organisation’s functions or activities may contravene the collection principle (IPP 1.1) and could be considered unreasonably intrusive or unfair under IPP 1.2 if done covertly.

**More information:** View [OVIC’s Guiding Principles for Surveillance](https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance/) and supporting [Case Study on using a communication platform to monitor employees](https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance/)