**SOCIAL MEDIA AND PRIVACY**

**FREQUENTLY ASKED QUESTIONS**

**CONTENTS**

[INTRODUCTION 3](#_Toc70001847)

[What is social media? 3](#_Toc70001848)

[ORGANISATIONAL USE OF SOCIAL MEDIA FOR BUSINESS PURPOSES 3](#_Toc70001849)

[What opportunities does social media bring to the public sector? 3](#_Toc70001850)

[What are some of the privacy risks associated with public sector use of social media? 3](#_Toc70001851)

[What does privacy law say about the use of social media by the public sector? 4](#_Toc70001852)

[There is so much information on social media. Does using social media mean our organisation is ‘collecting’ all of this information? 5](#_Toc70001853)

[What is the recommended process for organisations seeking to establish a social media presence that is consistent with privacy law? 5](#_Toc70001854)

[What about other considerations when using social media in the public sector such as freedom of information (FOI) and recordkeeping requirements? 6](#_Toc70001855)

[What protective data security considerations should an organisation take into account when using social media? 6](#_Toc70001856)

[My organisation wants to take photos of an event for its social media page. What privacy considerations are there? Do we need to obtain individuals’ consent to publish the photos online? 7](#_Toc70001857)

[My organisation wants to run an online competition and ask the public to make submissions through social media. What privacy considerations need to be taken into account? 7](#_Toc70001858)

[SOCIAL MEDIA, PRIVACY, AND THE WORKPLACE: EMPLOYERS 8](#_Toc70001859)

[How can organisations respond when an employee has misused social media in their personal life, or in the course of their work? 8](#_Toc70001860)

[Is there a privacy risk in accessing or monitoring employees’ personal social media accounts? 8](#_Toc70001861)

[Is there a privacy risk in accessing the social media accounts of job candidates as part of the recruitment process? 9](#_Toc70001862)

[What can organisations do to support employees using social media? 9](#_Toc70001863)

[SOCIAL MEDIA, PRIVACY, AND THE WORKPLACE: EMPLOYEES 9](#_Toc70001864)

[Is the personal information I post online protected by the PDP Act? 9](#_Toc70001865)

[How can I manage the relationship between my professional and personal life with regards to social media? 10](#_Toc70001866)

[I am my organisation’s social media administrator. What are the key privacy considerations I need to keep in mind? 10](#_Toc70001867)

[I believe my employer has been monitoring my activity on social media. What can I do? 11](#_Toc70001868)

INTRODUCTION

Social media is a useful way for public sector organisations to circulate information and engage with citizens, partners, and stakeholders. There are many factors that may deter an organisation from embracing social media – privacy is only one element. Other factors include unfamiliarity with the technology, lack of resources and infrastructure, and a culture of risk aversion.

The Office of the Victorian Information Commissioner (**OVIC**) supports the responsible use of social media throughout the public sector. Although there are inherent challenges associated with social media, organisations that adopt a risk management approach can establish a digital presence and enjoy its benefits while maintaining a strong commitment to privacy.

This document contains commonly asked questions regarding information privacy and social media in the Victorian public sector. It is intended to assist organisations that are unsure about how to use social media tools effectively while upholding information privacy under the Privacy and Data Protection Act 2014 (**PDP Act**). It is not a guide on how to use social media in general.

What is social media?

Social media is a broad term that covers a range of online services and tools. It can be used for publishing, sharing, and communicating information.

Some types of social media include forums, blogs, wikis, and social networking platforms that allow users to socialise and communicate online – for example, Facebook, Twitter and LinkedIn. Video and image sharing platforms such as YouTube, Flickr and Instagram also fall under the umbrella of social media, as does any other website or app that allows users to upload and share content.

ORGANISATIONAL USE OF SOCIAL MEDIA FOR BUSINESS PURPOSES

What opportunities does social media bring to the public sector?

Social media provides governments with effective tools to engage and communicate with citizens and stakeholders. The Australian Bureau of Statistics, Household Use of Information Technology, 2016-17 statistics note that approximately 80% of Australian internet users access the internet for social networking purposes. This clearly presents a significant opportunity for governments to reach a large proportion of the population.

When used responsibly and effectively, social media can:

* increase citizens’ access to government and encourage two-way communication;
* facilitate a sense of openness and trust in government;
* reach specific audiences on particular issues;
* create opportunities for marketing and promotion of government activities, services, and events; and
* allow governments to gain insight into emerging trends and issues of concern within the community.

What are some of the privacy risks associated with public sector use of social media?

There are several privacy risks to consider when using social media. However, when managed effectively before establishing a social media presence, these risks should not prevent an organisation from using and experiencing the benefits of social media.

Some of the common privacy risks that public sector organisations should be aware of include:

Over collection

The amount of personal information available on social media is immense, and organisations cannot control what other users disclose to them via this medium. As such, there is a risk that organisations may collect more personal information than is necessary for their functions.

One of the opportunities offered by social media is that it can facilitate a two-way channel of communication between organisations and the public. However, this also opens organisations up to comment from the public, which may increase the risk of over collection of personal information, including third party information.

While social media can create a dynamic form of communication, organisations should manage the way they interact with the public online, including having processes in place for how social media will be used. Some organisations may choose to focus on using social media as a way to broadcast information, rather than create dialogue.

**Remember**: Personal information on social media includes more than just an individual’s name. It may also include their profile picture, photographs containing identifiable individuals, geo-location, video and audio content, as well as personal opinions. Further, social media content may also have embedded information – for example, images may have metadata which could potentially identify an individual.

**Over sharing and permanency of content**

The nature of social media means that even if posts or accounts have been deleted, the information shared may remain archived or captured by others. It may also be shared further without consent, or even the original publisher’s knowledge; information has the ability to spread quickly via social media.

Because of this risk, organisations should be mindful of the permanence of what they post on social media and ensure they do not share information that is personal or sensitive in nature unless appropriate to do so.

Scams and malware

Social media involves interaction with a broad range of users, many of whom may be unknown to organisations. Clicking on links provided by unknown sources can give rise to risks such as phishing attacks and scams, or the introduction of malware into an organisation's system. This can lead to unauthorised access or disclosure of information, including personal information. It is therefore important to ensure that employees using social media are aware of these risks and take caution when clicking on links on other users' social media posts.

What does privacy law say about the use of social media by the public sector?

In Victoria, the Information Privacy Principles (**IPPs**) under the PDP Act govern the collection, handling, use and disclosure of personal information (excluding health information) by the public sector.

As principle-based legislation, privacy law in Victoria is technology-neutral. The IPPs are designed to be flexible so that organisations can apply them regardless of the technology they use or the projects they undertake – including establishing a social media presence.

As an example, IPP 1.3 requires organisations to take reasonable steps to provide notice to an individual when their personal information has been collected. Generally, this would mean a collection notice before or at the time of collection. However, within the context of social media, it may be appropriate to include an abridged version of a collection notice within the ‘About me’ or ‘Bio’ section of a social media profile, with further information available on organisations’ websites or in privacy policies.

For further information on collection notices, please refer to the Collection notices guidance available on the OVIC [website](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).

There is so much information on social media. Does using social media mean our organisation is ‘collecting’ all of this information?

Social media creates a unique environment for what constitutes ‘collection’ as traditionally understood in the PDP Act. Within an online context, merely seeing personal information of users on a social media platform (for example, of users that follow an organisation on Twitter) is, arguably, not considered to be collection under IPP 1.

For personal information to be considered as ‘collected’, it has to be held by an organisation. Organisations should only collect personal information from social media platforms if it is relevant to their functions. Once collected, that information must be handled in accordance with the IPPs.

What is the recommended process for organisations seeking to establish a social media presence that is consistent with privacy law?

The specific process for each organisation will differ according to their unique business context, including the type of social media they intend to use, and for what purpose.

In general, some steps to consider include:

1. **Assess which social media platform is best suited to the goals and priorities of the organisation.** Consider the balance between the needs of the organisation and the privacy risks associated with that particular platform.

Organisations should be aware of the terms and conditions of the social media platforms they sign up to. While organisations may handle personal information in accordance with the IPPs, a social media platform’s practices may not be consistent with these principles.

This is particularly relevant if the platform is based outside Victoria (see IPP 9). Terms of service policies or similar documents will generally include important information that may affect organisations’ ability to uphold the IPPs, such as who owns the data, and what happens to it if an account is deleted.

1. **Undertake a privacy impact assessment** **(PIA)** **of the program**. A PIA will assist organisations to identify any privacy risks associated with a particular social media platform, as well as potential risk mitigation strategies. OVIC’s [resources](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/) contain a PIA template and guide.
2. **Undertake a security risk assessment.** While a good PIA will touch on security, a stand-alone assessment of the security implications of social media use should be conducted, in addition to a PIA. See OVIC’s information security resources for more information on security risk assessment.
3. **Consider internal and external policies and procedures and whether they need updating to accommodate for social media use.** Creating a specific social media policy that includes guidance on appropriate use, security protocols, and clear lines of responsibility and accountability is recommended. Further, if organisations are collecting people’s personal information via social media, this should be accurately reflected in privacy policies and collection notices.
4. **Review the technical settings of the chosen social media platform and customise them where possible.** Default privacy settings on a platform will often be at the lowest level, so ensure the settings you choose reflect a high standard of privacy protection, and are consistent with the organisation’s privacy policy.
5. **Ensure employees with access to official social media accounts are properly trained.** This may include training on how to use the platform itself, appropriate use in line with the organisation’s social media policy, privacy and security requirements, and procedures to follow should a privacy or security breach occur. Organisations should appoint a social media administrator who is responsible for overseeing the organisation’s social media use. The administrator should be aware of the Information Privacy Principles.

What about other considerations when using social media in the public sector such as freedom of information (FOI) and recordkeeping requirements?

Organisations should be mindful of their recordkeeping obligations in relation to social media posts, for example, in accordance with any requirements under the *Public Records Act 1973*. Captured social media records may include the personal information of individuals and such records should be handled accordingly. For more information about recordkeeping obligations in relation to social media, please contact [Public Record Office Victoria](https://www.prov.vic.gov.au/).

A social media post may also create a public record that would be considered a ‘document’ subject to a potential freedom of information request. It is important that organisations are aware of their recordkeeping obligations in relation to social media posts, as this will impact upon what records an organisation holds, and subsequently, what documents may be requested under an FOI request.

What protective data security considerations should an organisation take into account when using social media?

Any personal information collected through social media should be handled in accordance with IPP 4, which requires organisations to take reasonable steps to protect the personal information they hold.

IPP 4 does not specify what constitutes ‘reasonable steps’, however the Victorian Protective Data Security Framework (**VPDSF**) and the accompanying Victorian Protective Data Security Standards (**VPDSS**) provide useful guidance that is designed to be adaptable to each organisation’s unique business context and risk appetite.

The VPDSS adopt a risk-based approach to protective data security and emphasise robust governance, and security across four domains: physical, personnel, ICT, and information security.

Part 4 of the PDP Act, which relates specifically to protective data security, requires organisations to adhere to the VPDSF and VPDSS in relation to all public sector data, beyond just personal information. Organisations using social media should keep in mind their broader data security obligations, regardless of whether or not personal information is handled.

My organisation wants to take photos of an event for its social media page. What privacy considerations are there? Do we need to obtain individuals’ consent to publish the photos online?

In general, IPP 1.3 requires organisations to take reasonable steps to make people aware of a range of matters when their personal information is being collected – this includes when taking photographs in which individuals may be identifiable.

When taking photographs of a large crowd, it may be sufficient to provide a collection notice on a sign or poster. However, it is best practice to take reasonable steps to ensure anyone who is clearly identifiable in a photo has consented to their image being publicly shared. This promotes a stronger sense of trust between organisations and the community.

Organisations should consider taking the following steps when taking photographs:

* ask for permission prior to taking someone’s photograph, and let them know that the image may be published online; and
* if photographs will be taken at an event, include a statement in the registration process, or place clearly visible signs at the entrance, to inform people that there will be photography at the event. It is appropriate to also give people the option to notify the organisation if they do not wish to be captured in photographs. Be sure to include details of how they can contact the organisation about this.

My organisation wants to run an online competition and ask the public to make submissions through social media. What privacy considerations need to be taken into account?

In this scenario the organisation will be collecting personal information from people in order to run the competition. The same obligations under the IPPs exist when using social media as with other means.

The information collected may vary depending on the type of competition. For example, for a photography competition the information collected may include a person’s name, profile photo, the photograph the entrant is submitting (which may contain the image of an identifiable person), and any data embedded in the image. In line with IPP 1, organisations should only collect the minimum amount of personal information necessary to run the competition.

Organisations should also take reasonable steps to ensure that individuals making submissions to competitions are aware of what will be done with their personal information. Including a reference to the privacy statement or privacy policy of the social media platform being used to facilitate entries is an important step.

**Remember**: Asking people for their personal information via social media is asking them to share their personal information with a broader online audience. It is good practice to give people the opportunity to enter the competition in an alternative way, such as via email, if they do not wish to publish their submission online for everyone to see.

SOCIAL MEDIA, PRIVACY, AND THE WORKPLACE: 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.

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.

Is there a privacy risk in accessing the social media accounts of job candidates as part of the recruitment process?

Searching for information about a job applicant on social media and using it to inform hiring decisions may be problematic. There are many risks associated with this practice that go beyond privacy – for example, if an organisation makes a hiring decision based on what is discovered on social media (even if the information is not collected) it may find itself liable for discrimination.

In addition to privacy concerns, a further question regarding the legitimacy of accessing candidates’ social media accounts relates to its validity and fairness as a selection tool. Information gathered from social media may not be accurate or up to date (IPP 3), or it may be available for some job applicants but not others, making it impossible to standardise this process across all candidates for a position.

In general, if an organisation intends to view social media accounts as part of the recruitment process, job applicants should be made aware upfront that information obtained from social media may be used in assessing suitability for the role.

Organisations should also carefully document what information they are collecting about each applicant, how they are collecting it and the extent to which it is being relied upon in the decision-making process.

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.

SOCIAL MEDIA, PRIVACY, AND THE WORKPLACE: 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.

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice.