Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Mobile apps and social media

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

This guideline is intended to assist Queensland government agencies[1] in ensuring their creation and use of mobile apps and social media complies with the privacy principles[2] in the *Information Privacy Act 2009* (Qld) (**IP Act**).[3] A failure to comply with the privacy principles can result in privacy complaints being made by individuals who believe their privacy has been breached.

1.1 What is personal information?

Personal information is any information about an identified individual or an individual who is reasonably identifiable from the information.[3]. All information that fits this definition is personal information, even if it does not seem sensitive or appears to be harmless, unimportant, or trivial.

Refer to ***Key privacy concepts and sensitive information*** for more information.

1.2 What do the privacy principles require?

The privacy principles require agencies to handle personal information in specific ways. This includes rules about what, and how, personal information can be collected, when it can be used and disclosed, and how it must be secured and stored.

[1] Unless otherwise specified, in this guideline agency includes a Minister.
[2] The Queensland Privacy Principles (QPPs) and overseas disclosure rules in section 33.
[3] in addition to other requirements for agencies' use of social media, for example, Queensland Government Principles for the use of social media networks and emerging technologies, Code of conduct for councillors in Queensland RTI and public records requirements and specific agency social media policies

They also include rules about when personal information can be disclosed outside of Australia, which may apply to apps and social media given the personal information is online and often hosted by overseas-based servers.

2.0 What are mobile apps

A mobile application or 'mobile app' is a software program designed to run on a smartphone, tablet computer or other mobile device. Mobile apps are increasingly being used as part of the government's delivery of services to the community.

2.1 Does the IP Act apply to mobile apps

Any system which involves the collection, storage, use or disclosure of personal information by a Queensland government agency (or its bound contracted service providers) is subject to the requirements of the IP Act, the Queensland Privacy Principles (QPPs) and the overseas disclosure rules in section 33. Because mobile apps potentially capture information about their users, privacy must be taken into account in both the app's design and the information provided to users.

2.2 Privacy challenges for mobile apps

Mobile app capabilities present unique challenges for privacy protection. Mobile apps have the potential to collect significant amounts of personal information about users, often without them being aware of the collection. Mobile apps may be able to access:

- the user's phone and email contacts
- call logs
- internet data
- calendar data
- data about the device's location[4]
- the device's unique IDs[5]; and
- information about how the user uses the app.

The scope of personal information which can potentially be collected, combined with the speed at which apps are developed and distributed, could result in the personal information of hundreds of thousands of users being collected in a short space of time.

2.3 Privacy considerations when developing mobile apps

Like any other project involving personal information, privacy should be included in the planning phase of an app's development. It will also be an important consideration for the entire life cycle of the app.

Some key privacy considerations are set out in the table below.

[4] Which will generally be the location of the device's user.
[5] Each mobile device can have a number of unique identifiers, including the International Mobile Station Equipment Identity number (IMEI), Wi-fi Media Access Control (MAC) address, Internet Protocol (IP) address and Bluetooth address.

Action	Relevant legislation
Complete a Privacy Impact Assessment as part of project planning. Consider and map the flow of personal information. This will help to identify privacy vulnerabilities in a systematic way.	
Consider what personal information is essential for the app. Consider whether the app needs to collect and use personal information to function, or whether it can be used anonymously or with a pseudonym. If it does, collect only as much personal information as you need. Do not collect personal information just because it may be useful or valuable in the future and be aware of the special rules when collecting sensitive information.	QPP 2-3
Tell people how the app will use personal information. During the installation, make sure users are reasonably aware of the matters listed in QPP 5, including what personal information the app is collecting and why, and anyone it will be shared with. It can be difficult to communicate this information effectively in the small screen environment. Consider strategies for giving an effective notice, such as layering information and putting important information up front, or using graphics, colour, or sound to draw attention to notices.	QPP 5
Consider how personal information will be stored and secured. The IP Act requires that personal information is protected from misuse, interference, loss and unauthorised access, modification, or disclosure. Ensure that the storage and security of any personal information collected through the mobile app is well planned, and that appropriate controls are in place on both the mobile device and backend systems that will store personal information. Security safeguards should be appropriate to the sensitivity of the information.	QPP 11
Have a clear and accessible privacy policy. Ensure you have a clear and accessible policy which enables users to evaluate what you propose to do with their personal information. Users should be able to access this information before deciding whether to download the app. Make sure your policy lets users know how they can access or amend their personal information, how they can delete the app or their subscription to the app, and what will happen to personal information already collected and stored.	QPP 1

Only use personal information for the purpose it was collected; only disclose personal information in permitted circumstances. Agencies may need to use and disclose personal information for an app to function. For example, location data may be required to deliver certain functions in a navigation or public transport app. Agencies may need to share personal information with another entity to provide the services offered by the app. Apps should generally only use personal information for the purpose it was collected, and only disclose to the individual it is about, except in limited circumstances. Agencies should monitor apps to ensure personal information is only used and disclosed in ways that are permitted by the IP Act and in accordance with their privacy policy.	QPP 6
Will personal information be disclosed out of Australia? The IP Act sets out additional requirements when personal information is disclosed outside of Australia. This includes the storage of personal information on servers outside of Australia. If the development or delivery of the app involves disclosing personal information outside of Australia, you will need to consider the obligations in section 33 of the IP Act.	Section 33 IP Act
Consider whether contractors will be engaged to perform any services which involve the transfer of personal information. If an agency plans to engage a contracted service provider to perform services connected with the development or delivery of an app, compliance with the rules about contracted service providers in the IP Act may be required.	Chapter 2, Part 3 IP Act
Consider the end of life of personal information Ensure that a plan exists for when the app is deleted, or subscription ends, taking into account public records and other legal obligations.	*Public Records Act 2002* (Qld) QPP 4 QPP 11
Plan for breaches and complaints Agencies should develop specific procedures for dealing with privacy breaches and complaints associated with their mobile apps.	Chapter 3A & 5 IP Act

3.0 What is social media

Social media are websites and apps that allow users to create and share content or to participate in social networking.[6] Some of the more common social media platforms used by agencies are Facebook, YouTube, Instagram, and LinkedIn.[7]

Checklist

The checklist at the end of the guideline will assist anyone who contributes to social media networks and sites in the course of their employment by a Queensland government agency to ensure that use complies with the privacy principles. It should be used alongside agency-specific guidelines and policies governing social media use.

Agency social media plays an important part in agency engagement with the community, however the nature of social media means its creation and use can have privacy implications. It is important that agencies build appropriate protections into their policies on social media use and retention of records.

3.1 What is the purpose of the social media account?

The intended use of the social media account will impact the privacy precautions an agency has to take. For example, a Facebook account intended only to communicate news updates or emergency alerts which is set to disallow direct messages will require fewer privacy precautions than a Facebook account that allows people to ask questions and receive answers.

It is important that agencies define the purpose and limitations of the social media account as part of determining what steps must be taken to ensure it complies with the privacy principles. Agencies may want to consider a privacy impact assessment[8] for social media accounts that are intended for more than just broadcasting information.

Social media policies

A social media policy that includes guidance on the handling and posting of personal information can be an important part of ensuring social media accounts are, and remain, privacy compliant.

3.2 Disclaimers and QPP 5 matters

When an agency collects personal information, it must take reasonable steps to make the individual aware of the relevant matters listed in QPP 5.2.

This obligation applies when collecting personal information directly from the individual and when it is collected from someone else. It does not apply to

[6] Queensland Government Principles for the use of social media networks and emerging technologies
[7] ibid
[8] See Overview of the Privacy Impact Assessment process.

unsolicited information, however when a social media account allows people to submit information to it, information they provide will generally be solicited.

Ideally, the QPP 5 matters will be posted on the social media account itself, but if the platform does not have sufficient space, it can be posted on the agency's website with a prominent link from the social media account. Agencies may also want to include this information in their privacy policies under a social media heading.

Refer to ***QPP 5 – Informing people when collecting personal information*** for more information.

Agencies will also need to include a disclaimer addressing the overseas disclosure of personal information, e.g., one that ensures individuals interacting with the account understand that by doing so their personal information will be disclosed out of Australia.[9]

Acceptable use policies: other people's personal information

An acceptable use policy, e.g. setting out what content will and will not be permitted, generally forms part of an agency's social media policy. Agencies may want to consider including in their acceptable use policy a request that people do not post the personal information of third parties.

3.3 Security of social media

Social media accounts should be secured with a strong password and only specifically authorised employees—familiar with the agency's privacy obligations and social media policies—should have access to those credentials. This will help prevent inappropriate or unauthorised personal information being posted to the account and help ensure personal information collected through the account is secured against unauthorised use and disclosure.

The privacy and security settings of the social media account need to be set to an appropriate level based on the purpose of the account. If the account is solely for one-way communication by the agency to the community, disabling direct or private messaging and/or disallowing commenting on posts may be appropriate. However, different settings will be required for an account that is intended to facilitate two-way communication, e.g. answering questions, and responding to issues.

Regardless of the account's purpose, any settings that allow the sharing of information with third parties, e.g. affiliated companies, or advertisers, even in a deidentified or aggregated form, should be set to 'off' where possible.

Refer to ***QPP 11 – security-deidentification-and-destruction of personal information*** for more information.

[9] This may not be necessary if the platform's servers are located in Australia. Refer to Disclosing personal information out of Australia for more information.

3.4 Posting personal information to social media

The nature of social media means it is often used to share personal information, e.g. stories about individuals or community groups or photos and videos taken by agency employees. Care must be taken to ensure all personal information is published in a privacy appropriate way.

Before posting personal information to social media, e.g. photos taken by agency officers at an event, the agency must ensure it is permitted to do so.[10] This will generally require identifying what the individuals were told/what they agreed to when the photos were taken or contacting them to ask for consent.[11]

Agencies should develop a photo/image consent form that covers online publication and/or posting to social media, to be used when agency officers are taking photos or videos. This will ensure that the agency has the appropriate authorisation to use those images online.

Keep personal information to a minimum

Personal information published on social media can be harvested and reused by anyone. This can lead to annoyances, such as targeted marketing, or more damaging outcomes, such as identity theft, fraud, or harassment.

Even when an agency has authority to publish personal information to its social media account, it should limit it to the minimum necessary to fulfill the purpose of the post.

3.5 Responding to social media enquiries

Many social media accounts are intended to provide a customer-centric platform through which people can interact with the agency and receive timely responses.

Given the immediacy of social media, and the general expectation that enquirers will receive a rapid response, social media activities should be conducted by staff who have relevant expertise. This includes knowledge of their agency's privacy obligations; care must be taken not to disclose personal information in breach of the privacy principles.

Enquiries which would require disclosing personal information, e.g. a comment asking for an update on the progress of the commenter's application, should not be answered, even if the message has been sent privately to the agency's account. This is because the agency has no way to verify that the person making the request is who they claim to be. Even though some platforms have a 'real name only' policy, that does not guarantee the identity of the enquirer. They should be advised to contact the agency in another way so their identity can be verified, and the requested update provided.

[10] Agencies will need to satisfy QPP 6 section 33, as posting to most social media platforms means the information will be disclosed out of Australia.
[11] See Key privacy concepts – consent and QPP 6 – use or disclosure.

Responding to more general enquiries, e.g. comments asking how long until an agency completes a current project or the opening hours of a pool, should not raise privacy issues as they do not require the agency to confirm or disclose personal information beyond what the enquirer has already posted, e.g. the name/username of the enquirer.

3.6 Use and disclosure of information acquired through social media

Personal information collected through social media must be dealt with in accordance with the privacy principles, the same as personal information collected through other channels. This means there are limits on what it can be used for and to whom it can be disclosed.

The general rule in QPP 6 is that personal information can only be used and disclosed for the purpose it was collected. This means that if someone asks a question through social media, providing their personal information to the relevant part of the agency so they can send them an answer directly, using the personal information to respond to the question would generally be permitted.

There are exceptions to this general rule, including for law enforcement purposes and to prevent a serious threat to an individual or the public. If information sent to a social media account reveals, for example, a potential breach of the law or that someone may be a threat to themselves or others, the relevant exceptions may be open to be relied on to take appropriate action.

Use of personal information needs to be limited to what is necessary to fulfill the purpose. This means, for example, if someone asks a policy question through social media and the agency's intent is to respond through the same channel, it would not be necessary to provide the identity of the enquirer to the part of the agency preparing the response.

See ***QPP 6 – Use or Disclosure*** for more information.

3.7 Personal social media accounts

This guideline relates only to official agency accounts, however there may be circumstances when an agency employee receives a communication on their personal social media account directed towards them in their official capacity. These should generally be redirected towards an official agency communication channel and steps taken to capture the message in the agency's recordkeeping system. Employees engaging in official business through their personal social media accounts must ensure they comply with the privacy principles. A failure to do so can result in a privacy complaint.

Personal accounts linked to agency employment

Some social networking sites such as Facebook and LinkedIn may display details about the user's employment on their profile page. Employees should carefully consider whether this information should be displayed. Employees

should not use their agency email address to register and log into personal accounts.[12]

3.8 Requests to access social media information

Social media records—including records of official business conducted through an employee's personal account—are documents of the agency. They may also be public records. Social media records can be applied for under the *Right to Information Act 2009* and may need to be retained in accordance with the *Public Records Act 2002*.

For more information, refer to ***Online and on your phone: processing access applications for social media, webmail and text messages*****.**

Checklist - is your use of social media privacy respectful?

	Yes	No
Have you set the privacy settings? Most social media provides the capacity for you to limit the audience with whom you share your posts. However, keep in mind that you have little to no control over what will happen to information once posted. If someone decides to re-publish your content, it may end up with people and in places that you would not have chosen. You should bear this potential in mind before you post personal information.		
Have you kept personal information in your post to a minimum? Personal information is increasingly a valuable commodity. Some uses - such as targeted marketing and advertising - can be annoying to individuals. Personal information can also be used for criminal purposes such as identity theft, fraud and harassment. Be aware of this potential when you post not only other peoples' personal information but also your own.		
Have you obtained the consent of others before posting their personal information? Consent is a strong privacy permission. You choose what you post on social media about yourself. You should not assume that other people would necessarily consent to your choice to post their personal information online. The test is not whether you consider the information is harmless, the test is whether the other person would have chosen to post this information themselves.		

[12] Unless it is required; Yammer, for example, only allows registration with an official email address.

	Yes	No
Do you know all the people in your social media group or network? While some social media sites require members to provide their real names, you shouldn't necessarily assume that people are who they say they are. Sometimes this disguise can mask a malicious intent. If you wouldn't declare your personal information to a crowded room of strangers why would you post the same information online? If you don't fully know or trust the people in your social media group, you should exercise the same caution online as you would in person.		
Would your agency agree to your post? Once personal information is posted online, it can never truly be recalled or forgotten. If you post something online for a work purpose, it not only reflects on you but also your agency. The IP Act allows an individual whose privacy has been breached to make a complaint against your employing agency. Before you post – ask yourself whether the information you are sharing is something your agency would approve of. Additionally, how would future employers view your posts?		

If you have answered **no** to any of the above questions, you should reconsider how you use social media and what personal information you are sharing.

If you have answered **yes** you are in a good position to post the information to social media.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published October 2024 and Last Updated 4 October 2024