Office of the Information Commissioner
Queensland

Information Sheet

INFORMATION SHEET - *Information Privacy Act 2009*

Managing your Privacy Online

The *Information Privacy Act 2009* (Qld) (**IP Act**) provides for the protection of personal information collected and held by Queensland government agencies and provides rules for what those agencies must and may do with personal information.

Queensland government agencies are increasingly providing access to information and services online. Interacting online can include:

- submitting an online form
- creating a user account to apply for or receive services
- making an online payment
- contributing to an online survey or consultation; or
- posting on an agency's social media page.

Interacting online with a government agency typically will require you to provide some personal information, such as your name, contact details or your credit card number.

While an agency has obligations under the IP Act to protect your personal information, it is also important that you are aware of what steps you can take to safeguard your personal information when interacting online. Protecting yourself online is about more than how you set up and use your computer or mobile device. It's also about being smart in what you do and the choices you make when using the internet.

This information sheet provides practical tips for protecting yourself online when interacting with a Queensland government agency, as well as tips for general internet use. For detailed advice on staying safe online, please see the Australian government online safety and security website: Stay Smart Online.[1]

Check how your personal information will be used

Collection notice

When you provide your personal information[2] to an agency the IP Act requires that the agency takes all reasonable steps to make you generally aware of certain information. This will usually happen through a 'collection notice' – sometimes called a privacy notice.

[1] Accessible from https://www.communications.gov.au/what-we-do/internet/stay-smart-online
[2] Personal information is defined in section 12 of the IP Act. It is a broad definition that encompasses any information about an individual who can be identified directly from the information, or whose identity can be reasonably ascertained by reference to other information.

The collection notice sets out why your personal information is being collected, the legislative requirement or authority for this collection (if any) and to whom the agency routinely passes on your personal information.

If you have any queries about the collection notice, you should contact the agency and seek clarification before providing any personal information.

Do you know everything you are signing up for?

Some online services require that you agree to their terms and conditions – for example, before you create a user account or download an app. Not only do the terms and conditions inform you of your rights and responsibilities when using that service, they will often explain how your personal information will be handled.

By agreeing to the terms and conditions, you are entering into a contract with the agency or business which may involve the ongoing collection, use or disclosure of your personal information. It is particularly important to read the terms and conditions when providing personal information to a private sector organisation. As private sector organisations may not be obliged to provide a collection notice, the terms and conditions are where you will find the purposes for which your information will be used (for example, whether your information will also be used marketing or promotional purposes) and to whom it will be given.

Website privacy statement

Most government agencies provide a 'privacy' link in the footer of their website. This page explains in broader terms how personal information collected through the website is used and disclosed. It may also explain how you can access and amend personal information held by the agency or how to make a privacy complaint.

The website privacy statement should tell you whether the agency's website uses cookies[3] and for what purpose. Cookies allow a website to 'remember' things such as what items are in your shopping cart or your login status.[4] Cookies are also commonly used to collect information about how the website is accessed[5] for the purpose of analysing how the website could be improved. While cookies can collect relatively sophisticated information about the device you use to access the website, your identity is not necessarily readily identifiable through this information.

[3] A cookie is a small text file saved within your browser when you access a website.
[4] For example, without cookies you would need to log back into your account every time you move to a new page, even though you are already logged in.
[5] For example, the type of browser you are using, or the date and time you visited the site.

Why do certain advertisements follow me from website to website?

A third party cookie may be created if the web page you open loads any content from another website, such as an advertising banner. This third party cookie is then used by the advertiser to track your visits to other websites on which they advertise and send you targeted advertising.

If you are uncomfortable with this, most browsers can be configured to block some or all cookies, or delete cookies that have already been set, but you should be aware that you might lose some functions of that website. One approach is to set your browser to accept cookies only from the website you are currently visiting, or to start by blocking all cookies, then allow cookies as needed for websites that you trust.

Other steps you can take are to set your browser to private mode, install do not track software and/or use an ad blocker utility – such as an 'add-on' feature for your browser.

Secure your computer or mobile device

Malware, such as viruses or spyware, is software designed to 'infect' a computer system to cause harm. Steps you can take to secure your computer against malware include:

- Install reputable security software that protects your computer from viruses, malware and spyware.[6]
- Use a firewall.
- Turn on automatic updates so that your operating system and security software routinely installs any security fixes as soon as they are available.[7]
- Renew your security software when the subscription is due.

Backing-up your data on a regular basis can also help you recover your information if a virus destroys your files, or your device is stolen or damaged or exposed to ransomware.[8]

Secure your internet connection

An unprotected internet connection can result in unauthorised use and potential harm unless certain steps are taken. If you use a modem or router:

- change the default administrator password for the device
- disable remote management
- prevent unnecessary incoming connections; and

[6] A firewall is a piece of software or hardware that sits between your computer and the internet and acts as the gatekeeper for all incoming and outgoing traffic. Firewalls can keep hackers out of your device and inhibit the activities of malware and viruses.
[7] Reputable software companies often issue free updates to their software to fix security and other problems. Known as patches, these fixes should generally be applied as soon as they are released.
[8] Ransomware is a type of malware where a ransom is demanded of the owner in order to remove the infection from the owner's device.

- disable unneeded services.

If you have set up a wireless network:

- change the default digital name of your wireless hardware, and default administration username and password of the wireless software
- turn on encryption; and
- restrict access to computers or devices that you nominate.

Public wi-fi hotspots

A 'wi-fi hotspot' is public wireless network that offers a shared internet connection. Even where the wi-fi hotspot is provided by a Queensland government agency, your personal information could still be at risk as public wi-fi access is by its very nature, an unsecured network.

Steps you can take to protect your personal information when using a public wi-fi hotspot include:

- Confirm the 'official' hotspot name and manually connect to it (do not let your device automatically connect to the first wi-fi hotspot in its list).
- Avoid conducting sensitive transactions, such as online banking.
- Look for https:// in the website address ('s' stands for secure) and a locked padlock in the browser window, as this shows that the website is using a secure connection.

Protect your passwords

Did you know that an expert hacker can crack the average password in under three minutes?[9] Steps you can take to protect the security of your online accounts include:

- Use a strong password that contains a combination of uppercase and lowercase letters, together with numbers or special characters. Ideally, you should change your password on a regular basis.
- Use different passwords for different sites, particularly for sensitive transactions such as online banking. If one account is compromised the others will not be vulnerable to hacking.
- Memorise your passwords or use password management software (many are free to use and only incur costs if you wish to access increased functionality).
- Never store your passwords in a file that is saved on your computer. Similarly, you should avoid using the 'remember my password' option when logging onto a website. Not only can other users who have access to your computer log in to your accounts, so can others if your computer is hacked or infected.
- Don't tell your password to anyone else. This includes friends, family or the agency with whom you have an online account. No reputable

[9] Source: http://www.instantcheckmate.com/crimewire/is-your-password-really-protecting-you/

organisation will ever ask you for your password in order to rectify a problem with your account.

I have received an email about suspicious activity detected on my account!

Phishing is a form of fraud in which the scammer tries to trick you into providing personal information, such as your login details, by masquerading as a reputable entity. Phishing emails are commonly associated with banks, however scammers have been known to target customers of government agencies to trick you into providing information that can then be used to steal money or gain other benefits.[10]

Although some phishing emails are poorly written and clearly fake, others can look real, using agency logos, 'spoofed' email addresses or links to genuine looking websites.

If you receive a message asking for personal information such as your username, password, or credit card details - never respond by replying to the message, clicking on the provided link or opening an attachment as this may install malware or direct you to a malicious website.

Instead, contact the organisation by telephone to confirm that the request is legitimate. Alternatively, you could contact the organisation by typing the address of their website directly into your browser and sending them an enquiry, or answer with a new email message using an email address that you have used before or trust.

Social networking safely

Many agencies use social media as a channel for service delivery and engagement with the public. If you choose to post a comment, think before you make your personal information public:

- Be aware that publishing your personal information can affect your privacy rights under the IP Act. Queensland government agencies are not required to comply with certain privacy principles if the information is related to or connected with what you published or gave for the purpose of publication.[11]
- Limit the amount of personal information you provide. Don't post information that would make you vulnerable – such as your telephone number or address – as people other than just the agency will be able to see the information you post.

[10] For example, the Australian Taxation Office website provides samples of known phishing emails and highlights the aspects that identify them as a scam, accessible from https://www.ato.gov.au/general/online-services/in-detail/online-security/how-to-verify-or-report-a-scam/#Emailscams.
[11] For more information, see OIC's Information sheet: Self-publishing and the privacy principles, accessible from https://www.oic.qld.gov.au/guidelines/for-community-members/Information-sheets-privacy-principles/self-publishing-and-the-privacy-principles.

- Always seek permission before posting information about other people, including family members or friends.
- Remember that it can be difficult to remove personal information once it has been published.

Are your 'privacy settings' appropriate and adequate?

Most social networking accounts include privacy settings. These settings set the rules for who can view your contact information, see what you post, and see what others post about you.

Many networks have default privacy settings which are applied when you create your account. In some cases, the default setting is the most open setting available and can allow a high degree of access to your personal information. It is important that you make sure each privacy setting is right for you.

The Office of the Children's eSafety Commissioner[12] provides a guide to popular social media sites and apps which explains the default privacy settings and how you can adjust them.

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

This information sheet is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 3 July 2013 and Last Updated 23 February 2016

Changes to legislation after the update date are not included in this document

[12] Accessible from https://esafety.gov.au/esafety-information/games-apps-and-social-networking