Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Securing personal information

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

Under the *Information Privacy Act 2009* (**IP Act**), agencies must comply with Queensland Privacy Principle 11 (**QPP 11**) when securing personal information. This includes taking reasonable steps to protect personal information from misuse, interference or loss, and unauthorised access, modification or disclosure.

The **QPP 11 – Security, deidentification and destruction of personal information** guideline explains the requirements of QPP 11. This guideline is intended to provide practical guidance on QPP 11's implementation.

1.1 Standards and policies

When implementing QPP 11, agencies should refer to relevant legislation, whole of government standards, regulations and policies that relate to information security, such as Information Standard 18 – Information Security (**IS18**). In some circumstances, compliance with such standards will be sufficient to satisfy QPP 11. In others, additional protections may be necessary.

For example, a network may be secured against outside access or infiltration, in accordance with IS18, but unless there are methods in place to control and monitor staff access, it is unlikely to comply with QPP 11.

Proper security of documents containing personal information is not limited to physical or technological security systems, but requires training, monitoring, and auditing.

2.0 Adequate security safeguards

The security measures that an agency takes to protect documents containing personal information should be proportionate and appropriate to the possible risk of a security breach and the level of harm that could result from a breach.

Some document collections may require more stringent protections, based on the sensitivity or extent of the personal information.

2.1 Need to know

The primary safeguard in protecting documents containing personal information is to limit access only to those who need to access it in order to do their jobs.

Steps should be taken to ensure that computer and physical files which contain personal information are not readily accessible to everyone in the agency. This is particularly relevant where agencies have implemented whole of agency electronic document management systems, creating a central repository or index of all electronic files.

Controlling access involves more than deciding who should be able to access information. Other matters may need to be considered, such as:

- Is it necessary to limit the amount or type of information accessible to specific officers depending on their role?
- What rights should authorised officers have to deal with the information? For example, should they have 'read-only' access, or should they be authorised to change, add, or delete information?
- How should they be permitted to use the information? In almost all cases people should not access agency held information for personal reasons.
- Is the information accessible to contractors? For instance, does the organisation outsource functions or activities that involve information handling, or otherwise allow the contractor to access the agency's premises or information technology systems?
- What access, if any, is granted to external users – persons or bodies outside of the agency and what safeguards are in place to protect the information? For instance, how many external users have access and to what extent? What protections or controls are in place to ensure the external users maintain the security of the information and to audit their access?
- Who in the agency is authorised to grant access to the information, and under what circumstances? Who is authorised to disclose information to third parties and on what basis? Are there clear criteria, protocols, or policies for determining who gets access, or who is authorised to receive information? Is authorisation granted by a suitably senior officer within the agency?
- To whom are authorised officers permitted to disclose the information? Is there a need to specify a list or class of persons or bodies who are authorised recipients? Conversely, are there persons or bodies to whom

information should not be given because, for example, doing so could endanger the individual the information is about?

- Which officers have full privileges for electronic information or are able to access all or most of the agencies' document collections? Has their number been kept to the minimum necessary?

2.2 Using audit logs

It is important that an agency be able to determine if its security has been breached and personal information has been accessed, used, modified or disclosed contrary to the IP Act. Effective auditing will record who has accessed personal information, when, and for what purpose, and can be used to both detect and deter misuse.

A visible audit process may also help to ensure that officers access personal information only for agency purposes, which will also help to deter misuse.

Tip

To be effective, audit logs or audit trails must be usable and used. Audits must be carried out and responsibility given to a person who can assess whether a potential breach has occurred.

Agencies need to be able to interpret the audit log to determine what they need to know. For instance, does the audit log readily reveal who has accessed what information, and when? It is necessary to know what was done with the information, such as whether it was simply read, or whether it was copied, forwarded, modified, or deleted.

2.3 Securing physical storage

Another aspect of data security is physical security, which is concerned with controlling access to places where information is kept. These can be places – buildings, rooms, file cabinets, compactus, or objects, a laptop computer, USB key, briefcase, or mobile phone. This involves assessing what physical barriers or practices can be used to prevent an unauthorised access, misuse, modification, use or disclosure.

Premises can be secured using a range of devices, such as locks on doors, swipe cards, security guards, access registers, keypads, or biometric readers. There may be multiple layers of authorised entry and access. For instance, a wide group of people may be authorised to pass reception and enter the building, a lesser number of people to a specific floor, and still fewer to the rooms where computer hardware or files are kept.

Where floor plans include lockable office and cubicle workstations a degree of privacy and security for personal information is available, as files could be left out and computer monitors could not be readily viewed by passers-by. However, where an office is open plan, and/or uses shared workstations and computers, consideration will need to be given to mitigating any privacy risks.

Examples

- adopting clean desk policies
- providing separate conference rooms in which to meet with visitors or other agency staff
- providing provide rooms in which to conduct sensitive interviews of telephone calls
- providing lockable cabinets in shared workstations for each staff member
- providing separate log-ins for shared computers, with secure workspaces for each staff member that cannot be accessed by other users who share the computer.

2.4 Shared facilities

If an agency shares premises with another agency or with an organisation outside of Queensland government, consideration should be given to the potential privacy and security risks. Sharing computer and other information facilities creates even greater privacy and security risks. Even where premises are being shared by different units within the same agency, there is still the potential for personal information to be accessed, viewed, and potentially modified, misused or disclosed by officers with no need to know the information.

Consideration should be given to, for example, designing file rooms to maintain limited access to those persons with a need to know. Network and computer servers can be partitioned or restricted so that access is limited.

Hint

Policies or work practices which provide guidance to staff who are working in offices shared with other units of the agency or units of government agencies, will help to ensure the shared space does not lead to potential breaches of the IP Act.

2.5 Information on portable devices

Where personal information is stored on equipment, such as computers, or portable devices, such as USB keys, the information needs to be secured, particularly where they are taken outside of agency premises.

Laptop computers

Upon leaving agency premises, or where they are stored insecurely in those premises, laptops can be lost or stolen. Safeguards should be used to ensure that, if the equipment falls into the wrong hands, the information on it cannot be accessed. At the minimum, password protection and data encryption should be considered. Agencies should also ensure that staff are trained on proper use of agency laptops, including what should and should not be stored on them. Policies should also set out what an officer should do if they lose a laptop or suspect its integrity has been compromised.

USB storage devices

USB keys, memory sticks, portable hard drives and many MP3 players provide a simple way to store large amounts of data in a highly portable format. It is for this reason that USB devices represent a privacy and security risk, especially as their capacity increases and price decreases.

They are often used without any encryption or password protection, and the ease with which large amounts of personal information can be copied to these devices may mean that staff do not consider the potential risks. Their small size makes them easy to lose or misplace.

Agencies should ensure that all personal information copied onto these devices is encrypted, and should adopt policies and procedures for the use of USB storage devices which address:

- the use of personal USB devices in agency computers
- what information is appropriate to be stored on USB devices
- the precautions that must be taken for the physical security of the device.

Mobile phones

Personal information stored in agency issued mobile phones – such as contact details, text messages, video message and photographs – may be subject to the IP Act. If the device is a smartphone, such as an iPhone or a Galaxy, there is even greater potential for it to contain information subject to the IP Act. Where an officer is using a personal mobile phone for agency business, agency information stored on it may also be subject to the IP Act.

Agencies should, as part of their mobile communication device strategy, assess the extent to which these technologies are used and whether security or privacy risks need to be addressed. Agencies should also ensure that staff are aware of their privacy and security obligations when using agency issued devices, and are given guidance about the appropriate use of the mobile phone for work-related messaging.

At the very least, password or PIN protection should be used to limit unauthorised access to the device and its contents.

2.6 Securing information during and after transmission

Emails

Emails are easy to send, instantaneous, and can have significant amounts of personal information attached to them. Emails being sent outside of the agency should not be considered to be secure. Information sent to an intended recipient can be intercepted or circulated to those with no authority or need to know it. Care should be taken to make sure that email addresses are accurate and up to date and unnecessary copying or forwarding should not be undertaken.

Online information

Great care needs to be taken when an agency collects or disseminates personal information over the internet. Computer or coding errors can result in unauthorised access or disclosure on a world-wide scale.

Tip

Once personal information is placed on the internet, it may be difficult – if not impossible – to retrieve it. Organisations such as Google, through its cache function, collect and store copies of websites. This information remains available on these sites, even if the owner of the website deletes the information from their own.

While there are methods by which this information can be removed, they can be complicated and cumbersome and, if an individual has copied and placed the information on a personal website, or stored it in their records, there may be no way for the agency to have it removed.

Agencies that are considering using the internet to collect or make available personal information should consider privacy and security at each stage – before, during and after collection or dissemination. Agencies should consider ways to reduce the likelihood that search engines can seek out the information or archives will store it. Special coding can be used to repel search engine robots and spiders, so the website is excluded from internet search engines, and agencies should have plans in place to deal with any breaches that occur.

3.0 Document protection

Agencies should ensure that officers understand their responsibilities and obligations under the IP Act by providing clear guidance about appropriate access, use and disclosure. They should provide copies of policies and procedures to officers and ensure they understand their obligations under the IP Act and the organisation's internal policies. Staff should be trained, and relevant information should be included on log-in screens and in handbooks, policies and procedures.

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 August 2024 and Last Updated 22 August 2024