Interpreting the legislation – *Information Privacy Act 2009*

Understanding the Information Privacy Principles – protection and security of personal information (IPP 4)

1.0 Overview

Information Privacy Principle (**IPP**) 4 relates to the security of personal information. It requires agencies to ensure that they apply appropriate protections to the personal information they *control*. This means that, even where documents are being held by another body or person, if the agency[1] has the ability to exercise control over them it must take the steps necessary to ensure they are protected.

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 instances, compliance with such standards will be sufficient to satisfy IPP 4 (1)(a) and (2). In others, additional protections may be necessary.

[1] In this Guideline references to an 'agency' include Ministers and bound contracted service providers, unless otherwise specified.

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 IPP 4.

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.

Example

- involve extensive amounts of personal information
- involve information about vulnerable persons
- involve sensitive information, such as racial and ethnic origin, political opinions, sexual orientation or criminal records
- carry a risk of identity theft or financial harm
- carry a risk of harm to a person's life, safety, liberty, reputation or livelihood.

3.0 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. IPP 10 and IPPs 1-3 should be considered when deciding who in an agency needs to have access to the information.

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?

4.0 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 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.

Hint

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.

5.0 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, a 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.

Example

- 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.

6.0 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 used 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.

7.0 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.

7.1 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.

7.2 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.

Hint

Agencies might consider disabling access to USB ports on computers unless the staff member is authorised to use an agency USB device. An American company went so far as to use hot glue to fill all USB ports, but this is likely going further than is necessary under IPP 4.

7.3 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.

8.0 Securing information during and after transmission

8.1 Facsimiles

Facsimiles do not simply generate a paper document. They are computers that send, receive and store data electronically. Increasingly, facsimile machines are being combined with scanning and copying functions, with increasing potential to store information. As such, agencies should apply similar protections to these multi-function machines (many of which have the capacity to email documents directly) as they do to computers.

When transmitting documents, there is potential for the information to be disclosed to more people than the intended recipient. If the wrong number or email address is used, personal information may be disclosed contrary to the IP Act.

If no record is kept of the numbers dialled or email addresses sent to, it may become impossible to determine to whom the information was accidentally disclosed.

Hint

Some steps which can help ensure security are:

- isolate the fax machine in a secure area, to ensure only authorised persons can read faxes containing personal or otherwise confidential information
- use cover sheets which indicate the total number of pages faxed, and inform the recipient that the remainder of a transmission contains personal information or is otherwise confidential
- confirm the number before dialling, including a periodic check of pre-programmed numbers, to ensure they are accurate and not out of date
- phone ahead to advise that a facsimile of a sensitive nature is coming
- check the confirmation report to confirm the accuracy of the destination number and the correct number of pages transmitted.

8.2 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.

Hint

Agencies can enhance and maintain the security of emails through a variety of means and they should consider the following steps:

- establish what personal information is permitted to be sent via unencrypted email, and whether alternative means of transmission, for example delivery by hand or by registered post, are more appropriate based on the sensitivity of the personal information.

- determine when and what level of encryption is to be used, having regard to any prior need to establish suitable arrangements, for example, by providing digital certificates.

- adopt an email disclaimer to warn all recipients that the contents of the email may contain personal information and that privacy should be respected at all times. It should set out what steps should be taken if the email is received by someone other than the intended

recipient, such as notifying the sender and confirming whether the errant email should be deleted.

8.3 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.

Hint

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,[2] 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.

9.0 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.

9.1 Loss

Information can be lost both in the sense that its whereabouts are unknown and in the sense that there has been a failure to preserve or maintain it. Loss includes intentional or inadvertent destruction. Loss can be temporary or permanent, partial or total.

[2] Wayback machine: www.archive.org/index.php, Google cache: www.google.com/intl/en/help/features_list.html#cached

Where an agency loses personal information, they should consider notifying the individuals the information was about. See the discussion below in section 5 on data breach notifications for more detail.

9.2 Unauthorised use, access, modification or disclosure or any other misuse

Access will include viewing information on a computer screen or reading a document on a file. Unauthorised access may occur where a public official uses their access privileges for personal reasons.

Example

- satisfy their curiosity about any person
- gain an advantage for themselves or any other person
- get access to information they would otherwise have to buy
- access the information for someone else.

Modification includes changing, removing or adding information.

Generally, disclosing information means causing any other person to know it by opening it up to view or revealing it. Unauthorised disclosures will include those disclosures that are not permitted under one of the grounds in IPP 11 or, where it would be authorised under IPP 11, the officer in question was not authorised to make such a disclosure.

Access, modification or disclosure of personal information may be regarded as unauthorised where the person:

- has no authority to access, modify or disclose the information, for example:
  - where there is a legal restriction on access, modification or disclosure
  - where the person is not employed by the agency and has no authority to deal with the information
  - where the person obtains the authority by fraud or deception
- exceeds their authority, for example, where the person goes beyond their limited authority:
  - to view more information than they are permitted to view
  - to make certain types of modifications they are not permitted to make
  - to disclose to persons or bodies they are not authorised to disclose to
- misuses their authority, for example, by accessing information they are entitled to access, but for an ulterior purpose or motive, such as disclosing information for personal financial gain.

9.3 Unauthorised disclosure and security breaches

Actions that breach IPP 11, which sets out when an agency may disclose information, may also be a breach of IPP 4, but only where the breach occurred because of a failure to properly secure the information. IPP 11 focuses on the activities of the agency in proactively disclosing the information, while IPP 4 focuses on preventing unauthorised disclosure by the agency and unauthorised access by people outside the agency.

Hint

Information may be inappropriately disclosed even where adequate protections have been put in place. Even where an agency takes steps to ensure that information is protected, these security precautions may have been circumvented or ignored, including ignoring training in appropriate ways of dealing with personal information, resulting in an unauthorised disclosure.

Careless, negligent or accidental disclosures may be a breach of both IPP 4 and IPP 11 where there were steps the agency could have taken to better secure the information, for example through better training, records management or auditing practices.

10.0 Security breach notification

IPP 4(1) sets out the protections an agency has to place on personal information. IPP 4(2) requires that those protections include security safeguards that individuals would reasonably expect the agency to provide.

One safeguard that may be necessary in the event of a disclosure in breach of IPP 4 is notifying the individuals whose information was the subject of the breach.

There are some basic principles and factors that an agency should consider when deciding whether to notify individuals that their privacy may have been breached. The rationale for making notifications, and the steps agencies should go through in coming to a decision about whether notification is warranted in particular circumstances, is discussed below.

One of the objects of the IP Act is to provide for the fair handling of personal information. The objects of the Act must be kept in mind when applying the Act. This means that, when considering the requirement of IPP 4(2), in some circumstances, agencies should notify affected individuals of data breaches involving their personal information.

10.1 Deciding whether to notify

When deciding whether or not the breach affects the individuals any agency should consider these factors within the context of the personal information and the circumstances of the breach:

- the potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved (referred to as the 'data subjects') or otherwise affected, having regarding to:
    - the nature of the information, in particular its sensitivity
    - the amount of information
    - the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online
    - any relationship between the recipient(s) and the data subjects
- the extent to which the data subjects may already be aware of the breach of their information privacy and be able themselves to minimise the harm.
- the potential for notification itself to cause reasonably foreseeable harm to the data subjects (or any other person), excluding potential harm to those responsible for the breach (such as damage to reputation, or exposure to disciplinary action or claims for redress or bad publicity.
- Whether, considering the points above, notification is reasonably likely to alleviate more harm than it would cause

11.0 Service providers

Under IPP 4(b), if an agency gives a document containing personal information to a person or body in connection with the provision of a service to an agency, it must take all reasonable steps to prevent unauthorised use or disclosure of the personal information.

See *Contracted service providers under the IP Act* for a detailed discussion of an agency's obligations with regard to contractors and service arrangements involving personal information.

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

This guide 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 30 June 2009 and Last Updated 19 July 2013

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