



IPA and RTI – Training Guide

Griffith University 2010

Aim of this training guide

- » To provide a brief overview of the Queensland Government's privacy legislation: Information Privacy Act 2009
- » To explain the 11 Information Privacy Principles in relation to the collection, storage, use and disclosure of personal information
- » To ensure staff are aware of and understand the Privacy Policy

Legislation

Information Privacy Act

- the University must comply with the Information Privacy Principles
- This Act grants a right to access documents to the extent the documents contain an applicant's **Personal Information**
- Personal Information “is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.”

Is it personal information? Questions to ask yourself

- Is the information or opinion about an individual?
- Could a person identify the individual from the information?
- Could someone find out to whom the information refers?

Examples of personal information

- Name
- Address
- Date of birth
- Phone number
- Education details
- Employment details
- Financial details

Personal Information

- the University collects a large amount of personal information
- Student/Employee/Research participants
- Patients of the Health Clinic
- Childcare/Family Day Care clients
- Off Campus Accommodation providers
- Vendors of goods and services to the University
- Tenants
- Official Visitors

Release of Personal Information

- Section 42 of the Act says personal information may be accessed or amended other than by application under the Act
- the University has administrative release processes in compliance with Information Privacy Principles

Privacy Principles-General Guide

- IPPs 1, 2 and 3 apply to the collection by the University of personal information for inclusion in a document or generally available publication
- IPPs 4, 5, 6, 7, 8, 9, 10 and 11 deal with the obligations of the University where the University has control of a document containing personal information

IPP 1—Collection of personal information (lawful and fair)

Do not collect unless—

- lawful purpose;
- purpose directly related to a function or activity of the University;
- necessary to fulfil the purpose or is directly related to fulfilling the purpose.
- the University must NOT collect personal information in a way that is unfair or unlawful.

IPP 2—Collection of personal information (requested from individual)

ONLY applies if the University ASKS a person for—

- (a) their personal information; or
- (b) information of a type that would include their personal information.

The University must take all reasonable steps to ensure the person is generally aware of—

- (a) the purpose of the collection; and
- (b) if the collection is by law— that it is by law and the law;
- (c) if the University usually discloses to an entity, the identity of the entity; and
- (d) if the University is aware that entity usually passes the information to another entity, the identity of that entity.

Not required if delivering an emergency service and little benefit in complying and person not expected to be made aware of this.

IPP 3—Collection of personal information

- Only applies if the University asks for the personal information.

Take all reasonable steps to ensure—

- (a) the information is relevant to the purpose of collection
- (b) is complete and up to date
- (c) the collection is not unreasonably intrusive.

IPP 4—Storage and security of personal information

Protect documents containing personal information against—

- (i) loss
- (ii) unauthorised access, use, modification or disclosure
- (iii) other misuse

If it is necessary to give a document to a person in connection with a service provided to the University, the University must take all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.

IPP 5—Providing information about documents containing personal information

Ensure a person can find out—

- if the University has control of any documents
- type of personal information
- main use of the personal information
- how to obtain access to a document containing their personal information

This is NOT required if, by an access law, the University is authorised or required to refuse to give that information to the person.

IPP 6—Access to documents containing personal information

- the University must give a person access to the document if the person asks for access

This is NOT required if—

- (a) the University is authorised or required by an access law to refuse to give access to the individual; or
- (b) the document is expressly excluded from the operation of an access law

IPP 7—Amendment of documents containing personal information

Take reasonable steps to ensure the personal information—

- is accurate
- relevant, complete, up to date and not misleading

If a person asks for their person information to be amended and the University does not agree and there is no legal decision or recommendation to the contrary then if asked by the person the University should attach to the document a note of the amendment asked for by that person

IPP 8—Checking of accuracy etc. of personal information before use by agency

Before the University uses personal information take all reasonable steps to ensure the information is accurate, complete and up to date.

IPP 9—Use of personal information only for relevant purpose

Only use those parts of the personal information that are directly relevant to fulfilling the particular purpose.

IPP 10—Limits on use of personal information

Lists when the University can use information for a purpose other than the purpose for which it was obtained—

- by expressly or impliedly agreement; or
- necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or
- is authorised or required by law; or

For use by a law enforcement agency and necessary to

- prevent, detect, prosecute etc a crime
- protect public revenue
- prevent, detect etc serious improper conduct
- preparation or conduct of court proceedings

(keep a note with the document of such use)

Directly related purpose

Is de-identified, necessary for research in public interest and not practical to obtain consent (no reasonable basis to believe can be identified)

IPP 11—Limits on disclosure

Do not disclose the personal information to an entity other than the person concerned unless—

- the person is reasonably likely to be aware it is usual to disclose that type of information to the entity
- there is expressed or implied consent
- it is necessary to lessen or prevent a serious threat to the life
- the disclosure is authorised or required under a law
- it is necessary for a law enforcement agency to prevent a crime etc. (make a note of this and place with the document)

all of the following apply—

- necessary for research or public interest statistics if
- de-identified
- not practicable to obtain expressed or implied consent
- the third party will not disclose to a fourth party.

Must ensure the third party does not use for a purpose other than the purpose for disclosure to the University

The University may disclose if the third party wants to use for their marketing PROVIDED impracticable to seek prior consent and etc can free of cost opt out of receiving further marketing material contact details of the entity are provided

WRITE WITH CARE

- If you will be embarrassed in the event a document, file note or written communication, is made public **DO NOT WRITE IT**
- e-mails may be disclosed under the Information Privacy Act and the Right to Information Act

Transfer of information outside Australia

The University may transfer an individual's personal information to an entity outside Australia ONLY if—

- (a) the individual agrees to the transfer; or
- (b) the transfer is authorised or required under a law; or
- (c) the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; **OR**

- (d) 2 or more of the following apply—
- (i) the University reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs
- (ii) the transfer is necessary for the performance of the University's functions in relation to the individual;
- (iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;
- (iv) the University has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs.

Service arrangement

- ***contracted service provider*** to the University agrees to provide services for the purposes of the performance of 1 or more of the University's functions; and
- the services must be provided either—
 - (i) directly to the University; or
 - (ii) to another entity on the University's behalf
- not be in the capacity of employee.
- the University must take all reasonable steps to ensure that CSP is required to comply with part 1 or 2 and part 3 of IPA, as if it were the University.
- the University must comply with subsection (1) only if—
 - CSP will in any way deal with personal information for the University; or
 - the provision of services under the arrangement will involve—
 - (i) the transfer of personal information to the University; or
 - (ii) the provision of services to a third party for the University.

Complaints about breaches of Privacy

Complaints are to be made in writing to:

The Privacy Contact Officer

Office of the Pro-Vice Chancellor (Administration)

Griffith University Nathan Qld 4111

or by emailing the Privacy Contact Officer at:

c.mcandrew@griffith.edu.au

Privacy in Practice

The following scenarios provide examples of how privacy principles are applied in the workplace.

Click [here](#) to access scenarios

Scenario 1. *Collecting information*

As part of his duties as a Program Convenor, Max is required to interview students about their suitability for admission into an honours program. To streamline the admission process, Max drafted a form to collect information (including personal information) from applicants.

Max also included other questions to collect information from applicants because in many interviews, students complained that they had to supply much of the same information to other elements of the University which was a waste of time and money. Staff from these elements often called Max, or he called them, to obtain any information they needed to complete their duties. Max decided that it was best that he obtain as much information from the applicant while they were there so that he could use that information in the future, rather than the applicant having to come back or to go to another element.

Is he doing anything that breaches the IPPs?

Click [here](#) for answer to Scenario 1

Scenario 2. *The photocopier technician*

Roger, a photocopier technician had been asked to repair a broken photocopier at the office. As he walks through the door he notices an unattended file lying open on a desk and reads it. Roger comments: "Hey, I went to school with this guy. I didn't know he was being counselled for a drug problem?"

After fixing the photocopier, he is asked to attend another area of the office whose photocopier has just broken down while copying a grievance matter against an employee of the agency.

The officer who was copying the file takes the opportunity to grab a cup of coffee and leaves Roger in the photocopy room while the photocopier cools down. While waiting, Roger flicks through the file and realises that the person against whom the grievance is made lives in the same street as him.

What IPPs have been breached and why?

Click [here](#) for answer to Scenario 2

Scenario 3. *Confirming details with a caller*

Mary works in the HR branch. She receives a phone call from a bank employee who needs the employment details of one of the University's employees to process a home loan application.

What should Mary do in this scenario?

Click [here](#) for answer to Scenario 3

Scenario 4. *At the conference*

Bill and Tom are two academics who conduct research in the same discipline. Whilst attending a conference, Bill and Tom discuss details of a complaint made by a member of the public against a member of the research team concerning an ethical issue. They do not use the name of the researcher or the member of the public however the person seated behind them gasps and they realise that the person appears to recognise the people involved from the personal information exchanged when discussing that matter.

Have any IPP's been breached in this scenario?

If so, which ones?

If you believe that the IPPs have been breached, what are the consequences of the breach?

Click [here](#) for answer to Scenario 4

Scenario 5. *Leaving a message*

Tom telephones a student at home about attending a misconduct hearing. The student is not at home, however the student's partner, Christine, answers the phone. She states she knows all about the misconduct hearing but asks for clarification of the allegations. When pressed, Tom provides further details. Tom feels comfortable about providing this information to Christine because she is the student's partner and she has already told Tom that she knows all about her partner's misconduct hearing.

Is there anything wrong with giving Christine this information?

Click [here](#) for answer to Scenario 5

Scenario 6. *Contracts*

Jo has been asked to draft a contract and uses an old contract as a template. Although the contract does not involve any financial outlay and is not resource intensive for the University, it is binding for three years and involves the University disclosing personal information to a private company.

Jo adjusts the contract to reflect the circumstances of the services to be provided. As the contract is for a minor matter Jo's manager doesn't see any need to refer it any further. The manager signs off on the contract.

Should privacy be considered when drafting a contract? Why?

Click [here](#) for answer to Scenario 6

Scenario 7. *The Birthday Card*

Brad works in a Student Administration Centre and Janet is a student. They know each other as they used to attend the same high school. Occasionally they get together at the University to have a coffee and a chat about mutual friends. Brad knows that Janet's birthday is coming up because Janet happened to mention that she'll be another year older in the near future. Brad decides to access the student information system to find out Janet's date of birth and home address. A few weeks later Janet receives a birthday card from Brad sent to her home address.

Has Brad breached any IPP's?

Click [here](#) for answer to Scenario 7

Answer to scenario 1

*The collection of personal information is covered by **IPPs 1, 2 & 3.***

IPP 1 states that you may collect personal information only by lawful and fair means and only if it is necessary for, or directly related to, a lawful purpose which is directly related to a function or activity of the agency. The purpose for which the information is collected is crucial. There must be a legitimate purpose for the collection of personal information. Unnecessary information must not be collected. Ask yourself is the information necessary for the purpose for which it is being collected? Can it be done without? Do we really need to know the person's marital status, religion, age, if he or she has children, if he or she was charged with an offence, address, or even his or her name.

In this scenario, only some of the information Max proposes to collect is necessary for or directly related to a lawful purpose of his element. Other information is superfluous to his needs and does not need to be collected. Other elements have a lawful authority to collect the information and only those elements should collect that information.

IPP 2 provides that when you collect personal information directly from a person and you ask the person for the information, you must ensure that the person knows why the information is being collected, whether or not the collection is required by law, to whom the Agency usually discloses this kind of information and whether or not that agency or person is likely to pass it on again.

When drafting the form Max should include a statement on the form or provide verbal advice to the applicant that tells them:

- *the purpose for which the information is being collected;*
- *if the collection of the information is authorised or required by or under law, the fact that the collection of the information is so authorised or required; and*
- *any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.*

IPP 3 states that when you collect information you must ensure that the information is relevant to the purpose for which you are collecting it, and that it is up-to-date and complete. The information you collect should not intrude unreasonably upon the personal affairs of the person from whom you are collecting it.

In this instance, there is a chance that Max might use the information he collected in the future, when the applicant's circumstances have changed, thereby using information which is not up-to-date or complete.

Click [here](#) to access Scenario 2

Answer to scenario 2

*In this instance, **IPP 4 (Security) and IPP11 (Disclosure) have been breached.***

***IPP 4** requires files to be held securely and protected against loss, unauthorised access, use, modification, disclosure or any other misuse.*

Leaving files where people who shouldn't have access can view them breaches this IPP. Files should never be left unsupervised for anyone to read.

Minimum security measures require files to be stored securely when not in use and not to be accessed by visitors who attend the office. If it is not possible to lock your files away, staff should ensure that they are turned over so identifying information is not visible. Use your screen saver or log out to avoid visitors accessing any data held on your computer. Never leave visitors alone with personal or confidential information.

The employee who allowed access to the file has breached IPP 4.

***IPP 11** sets out when personal information can be disclosed. When Roger reads the file, information has been disclosed to someone outside the University because Roger is not an employee of the University. The information has effectively been disclosed (albeit inadvertently) because Roger is not a University employee and the University has no knowledge and therefore no control over the use of the information. It does not matter that the disclosure is inadvertent or unintentional.*

Personal information can only be disclosed to another person or agency if:

- *the person concerned is aware that the disclosure would be made;*
- *the person has consented;*
- *the disclosure is authorised or required by law;*
- *the disclosure is necessary to prevent or lessen an imminent threat to the life or health of an individual; or*
- *the disclosure is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.*

Click [here](#) to access Scenario 3

Answer to scenario 3

IPP 11 sets out when personal information can be **disclosed** (outside the agency) to another person, body or agency. Under IPP 11, personal information can only be disclosed to another person or agency if:

- the person concerned is reasonably likely to be aware that information of this kind is usually passed to another person or agency;
- the person has consented;
- the disclosure is authorised or required by law;
- the disclosure is necessary to prevent or lessen an imminent threat to the life or health of an individual;
- the disclosure is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.

While the employee may have approached the bank for a loan, Mary doesn't know this. Mary should refuse to provide the personal information to the bank until she checks with the employee and obtains their consent to release the information. Mary should also ask the bank to fax her a request specifying what information they require. On receipt of the fax she should confirm with the employee that it is all right to release the employment details to the bank.

When providing information to the bank, Mary should take care not to include more information than was asked for.

IPP 8 relates to the **accuracy** of personal information. Personal information should not be used without taking reasonable steps to ensure that the personal information is accurate, up to date and complete.

Mary should ensure that the employee's details are up to date, relevant and complete by confirming them with the employee. She should make a note on the employee's record that she has confirmed the details with them.

Click [here](#) to access Scenario 4

Answer to scenario 4

IPP 4 (Security) and IPP 11 (Disclosure) have been breached.

IPP 4 requires files to be held securely and protected against loss, unauthorised access, use, modification, disclosure or any other misuse. This includes making sure that no one can overhear you when you are talking about confidential or sensitive matters. The University's Code of Conduct requires that staff not disclose any sensitive or confidential information gained through their official duties. University staff have a duty to keep such information confidential. By discussing personal information at a conference, Bill and Tom have breached IPP 4.

IPP 11 sets out when personal information can be disclosed.

Personal information can only be disclosed to another person or agency if:

- the person concerned is aware that information of this kind is usually passed to another person or agency;
- the person has consented;
- the disclosure is authorised or required by law;
- the disclosure is necessary to prevent or lessen an imminent threat to the life or health of an individual;
- the disclosure is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.

In this situation, personal information has been disclosed. It doesn't matter that the person being discussed wasn't specifically identified. It is enough if the context of the discussion enables the listener to identify the person.

The exemptions to IPP 11 do not apply to this scenario. This means that the employees have breached IPP 11. It doesn't matter that the disclosure is inadvertent and unintended.

Generally employees must not disclose such information to any person except where:

- there is lawful authority for the disclosure (ie. court evidence, duties under legislation);
- the information is officially available as a matter of public record (eg public registers); or
- the information was supplied to the agency for a purpose which permits its disclosure.

In these instances, employees must disclose only facts and should not express opinion on official policy or practice. There are mechanisms in place through which information can be obtained by members of the public, in particular, through the Information Privacy Act 2009 and the Right to Information Act 2009. Requests for information not normally available to the public should be referred to the Privacy Contact Officer.

Click [here](#) to access Scenario 5

Answer to scenario 5

*By divulging information such as the reason for the call (ie. that there is a misconduct hearing) and specific information about the nature of the allegation, Tom has breached **IPP11**. Christine may not know that her partner is the subject of a misconduct allegation, even though she professes to know all about the hearing.*

***IPP11** provides that personal information can only be disclosed to another person or agency if:*

- *the person concerned is reasonably aware that information of this kind is usually passed to another person or agency;*
- *the person has consented;*
- *the disclosure is authorised or required by law;*
- *the disclosure is necessary to prevent or lessen an imminent threat to the life or health of an individual;*
- *the disclosure is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue.*

*A better approach would be for Tom to provide his name and his contact details and ask that the student ring him as soon as possible. Tom shouldn't provide further personal information to a third party unless he has the consent of the individual or the disclosure falls within the exemptions to **IPP11**.*

Third party's include family members who may state that they have a right to know about the matter.

Click [here](#) to access Scenario 6

Answer to scenario 6

All new contracts, agreements, licences and MOU's and those due for renewal, must comply with the Information Privacy Principles (IPPs) where they involve access to personal information.

In this case, the University has agreed to disclose personal information to a private company to provide a service. As the contract used by Jo was an old template it may not have a privacy clause. Consequently the contract may not comply with the Information Privacy Act 2009.

In addition, an old contract is unlikely to include any records management provisions, any monitoring clause or any surviving obligations clauses. By using an old contract, the agency may not only breach the Information Privacy Act 2009 but may not have the power to seek any compensation or to terminate the contract should the contracted company use and disclose personal information contrary to the Act. Any inappropriate disclosure of personal information could cause a harm and embarrassment to the University and individual concerned.

To prevent this type of situation occurring, draft contracts should be assessed by the appropriate section in the University before being signed to ensure that relevant privacy clauses and draft privacy deeds (if applicable) are included in the contract.

Click [here](#) to access Scenario 7

Answer to scenario 7

*While the act of sending a birthday card seems fairly innocuous, Janet has every right to feel that her privacy has been breached. By using personal information which has been collected for a particular purpose (the administration of the University) and then using it for another purpose (obtaining a person's date of birth and address to send a birthday card), Brad has breached **IPPs 9 & 10 (Use)**.*

IPP 9. *Provides that personal information can only be used for a purpose to which it is relevant.*

IPP 10 *sets out when personal information can be used. Generally, personal information can only be used for the purpose for which it was collected and not for any other reason.*

When an agency collects personal information from its employees for its administrative processes (eg HR), the information cannot be used for another purpose unless;

- *the individual consents;*
- *the use is authorised by law;*
- *it is necessary to prevent or lessen a threat to the life or health of the individual;*
- *it is necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue or;*
- *the use is for a purpose directly related to the purpose for which the information was obtained.*

Brad has used Janet's personal information for a purpose other than the purpose for which it was collected. As a result, Brad has breached IPP 9.
