Policy

QPP PRIVACY POLICY

Policy statement

The Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism (DWATSIPM) (the department) takes the privacy of its customers and employees seriously, and is committed to respecting and protecting the privacy of their personal information by complying with its obligations under the *Information Privacy Act 2009* (Qld) (IP Act), including:

- the Queensland Privacy Principles (QPPs[1]) (Schedule 3)
- publishing a QPP Privacy Policy as required by QPP 1 (Schedule 3, Part 1, s1)
- developing a Mandatory Notification of Data Breach (MNDB) policy (Chapter 3A) (Part 6, s73), referred to as the Data Breach Policy
- maintaining a register of eligible data breaches (Part 6, s72)
- requirements about disclosure logs (s78B)
- ensuring information security arrangements in accordance with QPP 11 (Schedule 3, Part 4, s11)
- binding contracted service providers to comply with privacy principles provisions (Chapter 2, Part 3, s35 and s36).

Personal Information

Under section 12 of the IP Act, personal information is defined as:

> *'Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion–*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not'.*

Additional definitions of information privacy terms have been provided at **Appendix A**.

This QPP Privacy Policy will be reviewed every two years, or following times of significant organisational change, to ensure its continued relevance and appropriateness.

Further guidance about the QPPs and their application is provided by the Office of the Information Commissioner Queensland (OIC).

Objective

This policy aims to establish the obligations and principles of the department in complying with the QPPs under the IP Act. It also defines the roles and responsibilities related to managing and protecting personal information.

[1] *IP Act 2009 (Qld) Schedule 3*

Scope

In-Scope

The IP Act applies to agencies, which include departments and the Minister.

This policy applies to all DWATSIPM employees, and employees engaged on a temporary, part-time or casual basis, or on secondment from another department, as defined by the *Public Sector Act 2022 (Qld).* It also applies to other persons who perform work for the department including contractors, students gaining work experience and volunteers. For the purposes of this policy, the term contractor includes on-hired temporary labour services (agency staff).

Information Privacy – customer complaint

The IP Act defines how Queensland Government agencies manage the personal information they hold.

A complaint about a breach of privacy is in scope of the policy, however if the department makes a decision in relation to a Right to Information or Information Privacy application for access to documents, this is out of scope of this policy. These out-of-scope decisions include a decision to refuse you access to, or amendment of, documents, that no documents exist or can be located, or not to waive charges.

On receipt of an in-scope privacy complaint, the relevant business area must provide the Governance, Planning and Reporting (GPR) team with a copy of the privacy complaint and any relevant documents.

Section 18 of the IP Act provides that an agency means a Minister, a department, a local government, or a public authority. Although the term 'agency' includes a Minister, section 20 limits this to acts done or practices engaged in by the Minister in their capacity as a Minister in relation to the affairs of an agency they administer. Additionally, under section 38, an agency does not contravene the QPPs when it gives personal information to a Minister to inform the Minister about matters relevant to the Minister's responsibilities in relation to the agency.

Human rights – customer complaint

The *Human Rights Act 2019* (HR Act) requires the department to:

- deliver services in a manner compatible with human rights,
- consider human rights in all circumstances, and
- make decisions that are compatible with human rights.

If the complainant believes their human rights have been limited due to an action or decision of the department, or DWATSIPM employees, this will be investigated during the complaints management process. If the complainant does not mention a breach of human rights, but a potential human rights issue is described in the complaint, the department will initiate an investigation of the human rights issue.

Victim's rights – customer complaint

The *Victims' Commissioner and Sexual Violence Review Board Act 2024* (VCSVRBA) defines the rights of a victim which must be upheld by Queensland Government entities and provides direction on the reporting and referral of related complaints. A complaint about a breach of an affected victim's Charter Right, which is in line with the definition of 'victim' defined by the VCSVRBA (refer to **Appendix A**), is in scope of this policy.

If the complainant does not mention a breach of a Charter of Victims' Right, but a potential breach is described in the complaint, the department will initiate an investigation of the Charter of Victims' Rights breach. If a complaint is referred to another entity to deal with the complaint, and is identified as a Charter of Victims' Rights complaint, this must be captured within the complaints reporting.

Out-of-Scope

There are some documents to which the QPPs do not apply, including:

- generally available publications
- documents held in a library, art gallery or museum for reference, study, or exhibition

- public records under the *Public Records Act 2023* (Qld) in the custody of Queensland State Archives that are not in a restricted access period under that Act
- a letter, or anything else, while it is being transmitted by post
- a document to the extent it contains personal information:
  - arising out of, or in connection with, certain covert activity (e.g. operations under the *Police Powers and Responsibilities Act 2000* (Qld) or the *Crime and Corruption Act 2001* (Qld)
  - relating to witness protection under an Act
  - relating to disciplinary actions or misconduct (e.g. under *the Police Service Administration Act 1990 (Qld)*, the *Crime and Corruption Act 2001 (Qld)* or public interest disclosures under the *Public Interest Disclosure Act 2010 (Qld))*
  - regarding matters subject to the Cabinet and Executive Council exemption in the *Right to Information Act 2009* (Qld)
  - arising out of a commission of inquiry.

Principles

The 10 Queensland Privacy Principles (QPPs) cover the responsible collection, use and disclosure, storage and security, and access and amendment of personal information held by the department. The QPPs can be broadly aligned with the four information handling stages shown in Figure 1, and detailed further below:

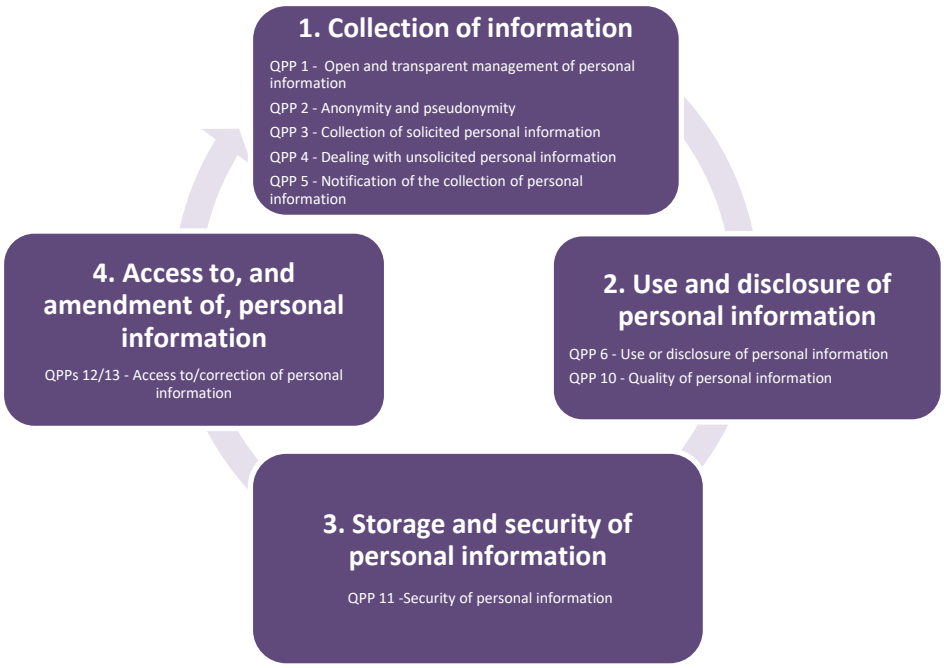

Figure 1: QPPs aligned with four information handling stages

1. Collection of information

QPP 1 — Open and transparent management of personal information

The department manages personal information in an open and transparent manner. It has policies, processes and systems in place to ensure compliance with the QPPs and to deal with any inquiries and complaints from individuals about the department's compliance. These policies include the QPP Privacy Policy which details how the department manages personal information.

Personal information collected and stored by the department

Personal information is collected by business areas throughout the department in the course of their day-to-day activities for statutory, regulatory and administrative reasons. Collection of such personal information is in accordance with QPPs 1 to 5.

The types of personal information that the department collects may include information about:

- clients, their family members and carers
- departmental employees, including prospective employees, and contractors
- representatives and employees of non-government service providers
- representatives of organisations, local governments and members of ministerial advisory committees that may be constituted from time to time
- vendors and service providers.

Departmental employees are given access only to information that is relevant to their duties and appropriate information security procedures are in place for the management of personal information.

Personal information is held on departmental files related to business and service delivery functions of the department, including delivery of the following responsibilities:

- Client relationship management / public correspondence to the Director-General and Minister
- Grant applications
- Award nominations
- Event programs
- Job applications, including recruitment and selection documentation
- Performance and Development Agreements
- Onboarding documentation
- Human resource management
- Policy consultation processes
- Cabinet documents.

The department also manages registers containing personal information, such as:

- Gifts Register
- Register of contact with Lobbyists
- Sponsorship Applications
- Function and Events Registers
- Communities and personal histories database
- Aboriginal and Torres Strait Islander Cultural Heritage Database and Register
- Corporate records / financial management records
- Consultant and contractor records.

Personal information may be stored in many formats, including hard copy (e.g. paper, photograph, video/audiotape) or electronic (e.g. in an electronic database or digital format).

The department may also deal with personal information in administering the following legislation:

- *Aboriginal Cultural Heritage Act 2003*
- *Torres Strait Islander Cultural Heritage Act 2003*
- *Aboriginal and Torres Strait Islander Communities (Justice, Land and Other Matters) Act 1984*
- *Multicultural Recognition Act 2016*
- *Integrity Act 2009*

Data collection methods

The data collection methods include online and paper-based data collection forms, written or computer records of telephone inquiries, and camera surveillance in government buildings for security and safety purposes. The

department uses cookies and web measurement tools to collect anonymous statistical data on website visits, including browser type, pages accessed, and IP addresses. This information is used for system improvements, not for identifying individuals. Email traffic may be monitored for troubleshooting, but personal details are not shared or added to mailing lists without consent, unless required by law.

Privacy complaint handling

An individual may make a complaint about a breach of the QPPs.

Privacy complaints must be made in writing within 12 months of the issue, using the Privacy Complaint Form (**Appendix B**), with proof of identity required. Once the form has been completed, it is required to be emailed to the Governance, Planning and Reporting team.

If you need help completing the form, please contact us by email privacy@dsdsatsip.qld.gov.au or by post:

> Manager, Governance, Planning and Reporting
> Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism
> GPO Box 806
> BRISBANE QLD 4001

If a complaint is unresolved after 45 business days, it can be escalated to the Office of the Information Commissioner (OIC). A guide outlining the privacy complaint process is available from the OIC website. If mediation through OIC is unsatisfactory, the matter may be referred to the Queensland Civil and Administrative Tribunal (QCAT) for a decision.

Contracted service providers and information privacy

Where the department enters into a contract or other arrangement for the provision of services relating to the performance of departmental functions which deal with personal information, the department must take all reasonable steps to bind the service provider to comply with the privacy principles. If the department does not do so, it may be liable for any privacy breaches by the service provider.

Disclosure of personal information overseas

The IP Act (s33) regulates the disclosure of personal information to entities outside Australia. This is relevant in circumstances such as where it is proposed that personal information be stored on computer networks and servers outside Australia, with the individual's consent.

For example, personal information may be disclosed to:

- **The United States of America**, through the use of platforms such as Meta (Facebook, Instagram), YouTube, LinkedIn, Microsoft Forms (survey tool), Vision6 (communication tool), Airtable (social media content planning tool), Canva (communication/media/design planning), Dropbox (file sharing platform), and Adobe.
- **Canada**, through the use of Hootsuite (social media publishing platform).

Availability of the QPP Privacy Policy

The department's QPP Privacy Policy is published on the department's website, and made available in other accessible formats, on request.

QPP 2 — Anonymity and pseudonymity

Individuals have the option of not identifying themselves, or of using a pseudonym, when dealing with the department in relation to a particular matter. However, this does not apply, if:

(a) the department is required or authorised under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the department to deal with individuals who have not identified themselves or who have used a pseudonym.

For most of our functions and activities, we need your name and contact information, and enough information about the particular matter, to enable us to fairly and efficiently handle your matter.

If the department is authorised to deal with identified individuals, it may have the discretion to allow individuals to remain anonymous or use a pseudonym. However, if the department is required by law to deal only with identified individuals, it does not have this discretion. Whether discretion can be exercised, and whether it is appropriate to do so, depends on the legal authority or requirement and the specific nature of the interaction.

Individuals may interact with the department anonymously or pseudonymously in certain situations, such as:

- Lodging a complaint: A person raising a complaint about a public service issue may not need to provide their identity for the complaint to be investigated.
- Making a submission: A person participating in a public consultation process may choose to remain anonymous or use a pseudonym, as their identity is not essential to the process.

QPP 3 — Collection of solicited personal information

Personal information other than sensitive information

The department collects personal information:

- that is reasonably necessary for, or directly related to, the one or more of the department's functions or activities
- lawfully and fairly
- from the individual, unless an exemption applies (including consent, lawful authority/requirement and law enforcement), or it is unreasonable or impracticable to do so.

The department does not collect sensitive information about an individual unless:

- the individual consents to the collection of the information
- the information is reasonably necessary for, or directly related to, one or more of the department's functions or activities
- the collection of the information is required or authorised under an Australian law or a court or tribunal order
- a permitted general situation exists in relation to the collection of the information by the agency, such as during a disaster event.

QPP 4 — Dealing with unsolicited personal information

Where the department has received unsolicited personal information, the information will be assessed to determine whether it could have been collected under QPP3 – Collection of solicited personal information, and/or whether it is a public record. If not, the department will, as soon as practicable, destroy or de-identify the unsolicited personal information, subject to public record laws and if it is lawful and reasonable to do so.

QPP 5 — Notification of the collection of personal information

As soon as practicable after the department collects the personal information about an individual, the department will take steps that are reasonable in the circumstances, to make sure individuals are aware of the matters listed in QPP 5 – Notification of the collection of personal information. This includes the

department's contact details, the fact and circumstances of the collection, whether the information was collected from someone other than the individual, the consequences if the information is not collected, and how the individual may access the personal information about the individual that is held by the department. This applies when personal information is collected from an individual or from a third party.

The department does not need to provide a formal QPP 5 notice. The QPP 5 matters can be communicated in other ways, such as informally or verbally.

2. Use and disclosure of personal information

QPP 6 — Use or disclosure of personal information

The department only uses and discloses personal information for the reason that it was collected, unless QPP 6 – Use or disclosure of personal information, allows it to be used or disclosed for a secondary purpose. This includes:

- instances where the individual has consented to the use or disclosure of the information
- QPP6 specific secondary purposes, including where:
  - the individual would reasonably expect the agency to use or disclose the information for the secondary purpose (subject to limitations)
  - it is required or authorised by law or reasonably necessary for law enforcement activities
- permitted general situations such as lessening or preventing a serious threat or locating a missing person (Schedule 4, Part 1 of the IP Act).

Where the department uses or discloses personal information in accordance with QPP 6, a written note of the use or disclosure needs to be made.

QPP 10 — Quality of personal information

The department takes reasonable steps to ensure that the personal information collected, or disclosed, is accurate, up-to-date and complete; and that the use or disclosure is relevant to the purpose of the use, or the disclosure.

3. Storage and security of personal information

QPP 11 — Security of personal information

The department takes reasonable steps to protect the personal information it holds from:

- misuse, interference or loss,
- unauthorised access, modification and disclosure.

Secure storage and handling of personal information is ensured through Threshold Privacy Impact Scans and Privacy Impact Assessments for relevant projects, clear procedures for breaches and complaints and strong governance mechanisms, including designated privacy roles. Staff receive mandatory privacy training, and compliance is reinforced through supervision, audits, and contractor obligations. Access to personal information is restricted to authorised personnel with a legitimate need.

Where personal information is no longer needed for any purpose and is not a public record, or otherwise required to be retained under law or court or tribunal order, the department takes reasonable steps to destroy or deidentify the personal information.

4. Access to, and amendment of, personal information

QPP 12, QPP 13 — Access to/correction of personal information

Access to personal information held by the department

Where the department holds personal information about an individual, the agency will, on request by the individual, give the individual access to the information.

Formal applications under the *Right to Information Act 2009* (Qld) are intended only as a last resort, and the department endeavours to provide individuals with access to their own personal information informally.

Individuals have the right to access their personal information held by the department, either through administrative access schemes or formal applications under the *Right to Information Act 2009* (Qld) (Qld). Access may be refused if restricted by law or if third-party information is involved. Individuals can also request corrections to their personal information to ensure accuracy, completeness, and relevance.

Correction of personal information

Where the department holds personal information about an individual, and has determined that the information is inaccurate, out-ot-date, incomplete, irrelevant or misleading; or where an individual has requested that the information is corrected, the department will take reasonable steps to correct the information.

If the department is authorised to refuse to correct or amend the information under the *Right to Information Act 2009* (Qld) (Qld), it may refuse to make the correction or amendment.

In addition to meeting the requirements of the IP Act outlined above, the department applies an ethical lens to the management of personal information in any situation not explicitly covered by the relevant legislation, regulation or policy. This is extended to information sharing with funded entities and third parties who are engaged to perform work on behalf of the department. This requirement includes meeting the obligations under s25 of the *Human Rights Act 2019* (Qld), which upholds the right of all people to not have their privacy unlawfully or arbitrarily interfered with.

Please note: The following QPP's are not used (i.e. the corresponding Australian Privacy Principles (APPs) were not implemented in the IP Act):

- *QPP 7 – Direct marketing*
- *QPP 8 – Cross-border disclosure of personal information, noting that similar requirements to APP 8 are contained in s.33 of the IP Act*
- *QPP 9 – Adoption, use or disclosure of government related identifiers.*

Artificial Intelligence

Artificial Intelligence (AI) solutions offer a range of opportunities for the department, including productivity, safety and accessibility benefits. To responsibly harness the benefits of AI however, privacy risks must be considered and appropriately managed.

Monitoring and Review

The department will monitor, review and update its QPP Privacy Policy and QPP Privacy Procedure, every two years or at times of significant organisational change, to ensure that they remain relevant and effective. Privacy is fast-moving and continues to evolve, requiring the department to be proactive and to anticipate future challenges.

Human Rights

The policy has been reviewed for compatibility with human rights under the *Human Rights Act 2019* (the Act). The policy was not found to engage any human rights under that Act. As such, it is reasonable to conclude the policy is compatible with human rights.

Authority

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Information Privacy and Other Legislation Act 2024 (Qld)

Invasion of Privacy Act 1971 (Qld)

Crime and Corruption Act 2001 (Qld)

Police Powers and Responsibilities Act 2000 (Qld)

Police Service Administration Act 1990 (Qld)

Public Interest Disclosure Act 2010 (Qld)

Public Records Act 2023 (Qld)

Public Sector Ethics Act 1994 (Qld)

Public Sector Act 2022 (Qld)

Human Rights Act 2019 (Qld)

Victims' Commissioner and Sexual Violence Review Board Act 2024 (Qld)

Delegations

Not applicable

Records File No:

Date of approval: July 2025

Date of operation: July 2025

Date to be reviewed: July 2027

Office:	Governance, Planning and Reporting
Help Contact:	Manager, Governance, Planning and Reporting privacy@dsdsatsip.qld.gov.au

---

Links:

Related Policies and Procedures

- QPP Privacy Procedure
- Data Breach Policy
- Data Governance Policy and Procedure (internal)
- Information Security Management System (ISMS) Directive (internal)
- DTATSIPCA Information Security Policy (internal)

- Information Security: Incident Response Plan (internal)
- Generative AI Guidelines (internal)
- Enterprise Risk Management Framework (internal)
- Enterprise Risk Management Policy (internal)
- Enterprise Risk Management Procedure (internal)
- Queensland Government – Information Security Policy (IS18:2018) (internal)
- Records Governance Policy (internal)
- Records Governance Procedure (internal)

Related Standards

- Queensland Government Information Standard (IS44 Information Asset Custodianship)
- Queensland Government Information Standard (IS18 Information Security Management System)
- ISO/IEC 27001:2022 – Information security management systems
- AS ISO 31000:2018 Risk Management – Guidelines

Appendix A – Definitions

Term	Meaning
Affected individual	Under section 47(1)(a)(ii) and (b)(ii), an 'affected individual' is someone: • to whom the personal information relates, and • who is likely to suffer serious harm as a result of the data breach.
Agency	Under the IP Act (S18), an agency means— (a) a Minister; or (b) a department; or (c) a local government; or (d) a public authority.
Disclose	Section 23 (1) of the IP Act, defines the disclosure of personal information as: (1) An entity (the ***first entity***) ***discloses*** personal information to another entity (the ***second entity***) if— (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.
Eligible data breach	For a data breach to be an 'eligible data breach' triggering notification and other obligations under the Mandatory Notification of Data Breach (MNDB) scheme, both of the following must apply: • there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and • the unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').
Information privacy	Information privacy refers to the position, policies, processes, and practices that protect the personal information of individuals. The department must comply with the 10 QPPs as set out in the IP Act.
Permitted general situations	Allows an agency to collect, use, or disclose personal information without consent in specific circumstances, including: • *Serious Threats:* If obtaining consent is unreasonable or impracticable, and the agency reasonably believes the action is necessary to prevent or lessen a serious threat to an individual's life, health, or safety, or to public health or safety. • *Unlawful Activity or Misconduct:* If the agency suspects serious unlawful activity or misconduct related to its functions and reasonably believes the action is necessary to take appropriate action. • *Locating Missing Persons:* If the agency reasonably believes the action is necessary to assist in locating a missing person and complies with relevant guidelines. • *Legal Claims:* If the action is reasonably necessary for establishing, exercising, or defending a legal or equitable claim. • *Alternative Dispute Resolution:* If the action is reasonably necessary for a confidential alternative dispute resolution process.

Term	Meaning
	These provisions ensure that personal information can be handled in exceptional cases where it is necessary and justified, while still adhering to privacy principles.
Personal Information	Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion– (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Privacy complaint	Under IP Act s164: (1) A privacy complaint is a complaint by an individual about an act done or practice engaged in by a relevant entity in relation to the individual's personal information that may be a breach of the relevant entity's obligation to comply with— (a) the privacy principle requirements; or (b) for an agency—chapter 3A, part 2 or 3. (2) However, a privacy complaint does not include a complaint in relation to the individual's personal information to the extent the personal information is— (a) in a document to which this Act does not apply; or (b) if the personal information is held by a bound contracted service provider—in a document held by the provider other than for the purpose of performing its obligations under the provider's service arrangement.
Responsible person	Under the IP Act Schedule 5, a responsible person is: (a) a parent of the individual; or (b) a child or sibling of the individual if a health professional believes the child or sibling has capacity; or (c) a spouse of the individual; or (d) a relative of the individual if the relative is a member of the individual's household; or (e) a guardian of the individual; or (f) a person exercising a power under an enduring power of attorney made by the individual that is exercisable in relation to decisions about the individual's health; or (g) a person who has sufficient personal interest in the health and welfare of the individual; or (h) a person nominated by the individual to be contacted in case of emergency.
Sensitive information	Personal information includes sensitive information, which is a specific category of personal information defined in schedule 5 IP Act. Sensitive information is information or an opinion about an individual's: • racial or ethnic origin • political opinions • membership of a political association • religious beliefs or affiliations • philosophical beliefs • membership of a professional or trade association • membership of a trade union • sexual orientation or practices • criminal record • health information • genetic information that is not otherwise health information • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.

Term	Meaning
Serious harm	Serious harm to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example— (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or (b) serious harm to the individual's reputation because of the access or disclosure.
Use	Section 23(2)(3)(4) of the IP Act, defines the **use of personal information** as: (2) An entity ***uses*** personal information if it— (a) manipulates, searches or otherwise deals with the information; or (b) takes the information into account in the making of a decision; or (c) transfers the information from a part of the entity having particular functions to a part of the entity having different functions. (3) Subsection (2) does not limit what actions may be ***use*** of the personal information. (4) However, ***use*** of the personal information does not include the action of disclosing the personal information to another entity.
Unsolicited Information	Personal information received by an agency that the agency took no active steps to collect; that someone has given or sent to an agency at their own instigation.
Victim	A victim is a person who suffers harm.

Appendix B – Privacy Complaint Form

Use this form if you want to make a complaint under the *Information Privacy Act 2009* about how your personal information has been handled by the Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism (the department).

What is a privacy complaint?
A privacy complaint is a complaint about how your personal information has been collected, managed, used or disclosed by the department.

> Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion–
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

(Section 12, Information Privacy Act 2009).

Can I make a complaint on behalf of someone else?
You can make a privacy complaint about how the department has handled *your own* personal information. If you contact us with a concern about how the department has handled the personal information of another person, we will assess the information you provide but may not be able to provide you with any feedback.

Privacy complaints can also be made by:
- parents on behalf of their children
- authorised representatives.

If you are acting for someone else, we will need evidence of your identity and your authority to act before we can give you any feedback.

Need help or advice about your complaint?
If you need advice about privacy concerns, please email the Manager, Governance, Planning and Reporting during office hours at privacy@dsdsatsip.qld.gov.au.

Privacy notice:

The Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism, is committed to handling your personal information in accordance with the *Information Privacy Act 2009* (Qld) and the Queensland Privacy Principles (QPPs).

QPP 5 – Notification of the collection of personal information, obliges us to advise you of certain matters when collecting your personal information. This collection notice sets out those matters, and explains how we will manage the collection, use, disclosure and storage of your personal information.

The information collected is necessary to assess and manage your complaint

Your personal information has been collected under authority of *Information Privacy Act 2009* (Qld).

If you choose not to provide your name and contact details it may prevent or reduce our ability to respond to your complaint.

We have collected your personal information through this form to appropriately manage and investigate your complaint. We may also request additional information if necessary to support the investigation.

• Your personal information will not be disclosed to any other agency. Should it become necessary to disclose your information to another agency, you will be notified.

• Your personal information will not be disclosed outside of Australia. Should it become necessary to disclose your information outside of Australia, you will be notified. Our privacy policy explains how you may request access to, and/or correction of, your personal information. Our policy also explains how you can complain to us if you consider we have breached our obligations to manage your personal information in accordance with the QPPs, and how we deal with privacy complaints. If you have questions regarding how your personal information will be handled contact us at: privacy@dsdsatsip.qld.gov.au.

1. Complainant's details			
Given name(s):		**Family name:**	
Address:			
Email:			
Daytime telephone:		**Other telephone:**	
Preferred method of communication	☐ Phone	☐ Email	☐ Post

2. Complainant's authorised representative's details (complete only if relevant) If you are acting for someone else, you must provide evidence of your authority to act, evidence of your identity and evidence of the complainant's identity (e.g. your driver's licence and your infant child's birth certificate).			
Given name(s):		**Family name:**	
Organisation:			
Address:			
Email:			
In what capacity are you authorised to act for the complainant?	☐ Parent of a child under 18 years ☐ Guardian ☐ Legal representative ☐ Power of Attorney ☐ Support service Other (please specify): _____		

3. How do you believe that your privacy has been breached? Please describe the conduct by the department you wish to complain about. We need to know what it has done, when the incident occurred, who was involved and how you believe your privacy was breached.
When did it occur?
What happened?
Who was responsible?
Where did it happen?

4. What impact has the privacy breach had on you?

5. What outcome are you seeking?

6. Signature and declaration	
I declare that: • the information provided in this form is complete and correct • I have read the privacy notice • where applicable, I have attached documents required for the purpose of this complaint (e.g. evidence of identity, or authorisation to act on another person's behalf).	
Complainant's signature *(or signature of authorised representative)*	
Date:	

7. Documents
Please provide copies of any documents that you think might help us look into your complaint (for example, letters or emails to or from the department). If you are making a complaint on behalf of another person, when you submit this form, please include a certified copy of your authority to act for the person for whom you are making the complaint, and evidence of your identity and that of the person for whom you are acting. If you have any queries about what is sufficient evidence of your identity or your authority to act, please email the Manager, Governance, Planning and Reporting at privacy@dsdsatsip.qld.gov.au.

8. Submitting this form
Please send the completed form and any relevant documents to privacy@dsdsatsip.qld.gov.au or Manager, Governance, Planning and Reporting Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism PO Box 806 Brisbane QLD 4001