Customer Contact **1300 COUNCIL (1300 268 624)**
07 4679 4000
www.**wdrc.qld.gov.au**
info@wdrc.qld.gov.au

Information Privacy- Council Policy

Effective Date	Ordinary Meeting of Council - 4 August 2010
Policy Owner	Customer Support and Governance Manager
Link to Corporate Plan	Strategic Priority: Financial Sustainability
Review Date	March 2020
Related Legislation	*Local Government Act 2009* *Information Privacy Act 2009* *Right to Information Act 2009* *Privacy Act 1988 (Cwth)*
Related Documents	Complaints Management - Council Policy Western Downs Regional Council Privacy Statement *Data breach notification - A guide to handling personal information security breaches* and the *Guide to developing a data breach response plan* - Office of Australian Information Commissioner

Policy Version	Approval Date	Adopted/Approved
1	4 August 2010	Ordinary Meeting of Council
2	6 May 2015	Ordinary Meeting of Council
3	21 March 2018	Ordinary Meeting of Council

This policy may not be current as Council regularly reviews and updates its policies. The latest controlled version can be found in the policies section of Council's intranet or Website. ***A hard copy of this electronic document is uncontrolled.***

1. PURPOSE

The protection of personal information which can identify an individual is a matter of great significance to Council and Council is therefore committed to protecting the privacy of individuals.

To ensure this protection, Council will take all reasonable steps to ensure that the collection, use, disclosure and handling of personal information complies with all relevant legislation, particularly the Information Privacy Principles contained in the *Information Privacy Act 2009.*

Further, Western Downs Health Services collects records and maintains a variety of personal information to enable effective service delivery and to meet business requirements. Western Downs Health Services ensures that all information is maintained, used and stored in accordance with the *Privacy Act 1988* (Cwth), including the Australian Privacy Principles contained therein.

2. SCOPE

This policy applies to all personal information held by Western Downs Regional Council. All Councillors and Council officers are responsible for ensuring this policy is understood and adhered to at all times.

3. POLICY

The *Information Privacy Act 2009* details how Council must handle personal information. The Act enables the right of individuals to request a copy of their personal information and to request documents to be amended if they are inaccurate or out dated, unless it is contrary to the public interest to do so.

In assessing whether it is in the public interest to disclose personal information, Council will consider the following factors detailed in the *Information Privacy Act 2009*, namely factors that:-

- are irrelevant to deciding the public interest;
- favour disclosure in the public interest; and
- favour non-disclosure in the public interest.

Openness

Council's Information Privacy Policy will be made available to the public free of charge on request and on Council's website.

The type of personal information held by Council includes (but is not limited to):-

- name and address;
- telephone numbers;
- email address;
- age and/or date of birth;
- property ownership and/or occupier details;
- library membership
- animal ownership;
- payment history; and
- pensioner and concession details.

Disclosure of personal information is only made after prior written consent of the individual is obtained or for the purposes stated in the collection notice.

Disclosure of personal information by placement on Council's website will be treated in accordance with Section 33 *Transfer of personal information outside Australia* of the *Information Privacy Act 2009*, whereby:-

- the individual gives prior written consent for their personal information to be placed on Council's website; or
- the placement of personal information on Council's website is authorised or required under a law; or
- where Council is satisfied there is reasonable grounds that the transfer is required to lessen or prevent a serious threat to life, health, safety or welfare; or
- in accordance with section 33(d) of the *Information Privacy Act 2009*.

Sensitive Information

Council will not collect sensitive information about an individual unless:-

- consent is provided by the individual;
- collection is required by law;
- collection is necessary to lesson or prevent a serious threat to life, health, safety or welfare of an individual; or
- collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

Anonymity

Council may, wherever it is practicable and lawful, offer individuals the option of not identifying themselves when entering into transactions with Council, however Council's ability to respond, action and/or provide a requested service may be limited.

Information Privacy Principles

IPP 1 - Collection of Personal Information - Lawful and Fair

All personal information collected by Council will be used only for the purpose of conducting Council business and for the provision of services to the community.

Council will only collect personal information in a lawful and fair manner for a purpose directly related to and necessary to fulfil a function or activity of Council.

IPP 2 - Collection of Personal Information - Requested from an Individual

When Council requests personal information or information of a type that would include the personal information from an individual, it will take all reasonable steps to ensure that the individual is generally aware of the purpose of the collection.

Council will advise the individual if the collection of the personal information is authorised or required under a law and the applicable law authorising the collection.

Council will also advise the individual if their personal information will be disclosed to another entity and the name of that entity either before the personal information is collected or as soon as practicable after the personal information is collected.

IPP 3 - Collection of Personal Information - Relevance

Council will take all reasonable steps to ensure that personal information collected is relevant to the purpose for which it is collected, is complete and up to date. The collection of personal information will not be done in a way that is an unreasonable intrusion into the personal affairs of the individual.

IPP 4 - Storage and Security of Personal Information

All reasonable steps will be taken to protect the personal information Council holds from loss, unauthorised access, use, modification, disclosure or any other misuse.

Council will take all reasonable steps to prevent unauthorised use or disclosure of personal information by service contractors contracted for the provision of a service to Council.

Document Set ID: 1205112
Version: 7, Version Date: 12/04/2018

Information is stored on Council's databases which are protected by passwords and other security measures with back-up copies stored at off-site facilities.

IPP 5 - Providing Information about Documents Containing Personal Information

Council will take all reasonable steps to ensure that a person can find out whether it has control of any documents containing personal information, the type of personal information, the main purpose which the personal information is used and how an individual can obtain access to a document containing their personal information.

IPP 6 - Access to Documents Containing Personal Information

An individual may request in writing access to their own personal information under the *Information Privacy Act 2009*. Council will provide access to requested information unless it is authorised or required under an access law to refuse to give the access the individual is seeking or the document is excluded from the operation of an access law. Suitable identification must be provided prior to an individual accessing the requested documents.

IPP 7 - Amendment of Documents Containing Personal Information

Council will amend documents containing personal information if requested by an individual if the documents are shown to be inaccurate, incomplete or out of date, however formal application under the *Information Privacy Act 2009* may be required.

IPP 8 - Checking of Accuracy of Personal Information before Use by Council

Council will take all reasonable steps to ensure that the personal information it collects uses or discloses is accurate, complete and up to date.

IPP 9 - Use of Personal Information only for Relevant Purpose

Council will only use the parts of personal information that are directly relevant to fulfilling the particular purpose for which it was collected.

IPP 10 - Limits on Use of Personal Information

Personal information collected by Council for a particular purpose will not be used for another purpose unless:

a. all reasonable steps are taken to obtain the written consent of the individual to use their personal information for another purpose; or
b. Council is satisfied that the use 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
c. use of personal information for another purpose is authorised or required under law; or
d. Council is satisfied that use of the personal information for another purpose is necessary for:
    i. the prevention, detection, investigation, prosecution or punishment of criminal offences of breaches of laws imposing penalties or sanctions;
    ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
    iii. the protection of the public revenue;
    iv. the prevention, detection, investigation or remedying of seriously improper conduct;
    v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.
e. the other purpose is directly related to the purpose for which the information was obtained; or
f. the use of the personal information is necessary for research or the compilation or analysis of statistics in the public interest; does not identify any particular individual the subject of the personal information; and it is not practicable to obtain the agreement of each individual the subject of the personal information before the use.

IPP 11 - Limits on Disclosure

Council will not disclose personal information to a person, body or agency (other than the individual concerned) unless:-

a. the individual concerned is reasonably likely to have been aware, or made aware under IPP 2, that information of that kind is usually passed to that person, body or agency; or

b. the individual concerned has consented to the disclosure; or

c. Council believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health safety or welfare of an individual, or to public health, safety or welfare; or

d. the disclosure is required or authorised by or under law, or

e. the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty or for the purpose of the protection of the public revenue, Council shall include in the record containing that information, a note of the disclosure.

A person, body or agency to whom personal information is disclosed under clause a. of this principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Council will ensure that disclosure of personal information does not occur unless the disclosure is for the purpose of distributing materials for and on behalf of Council, or when a third party has been contracted by Council for the sole purpose of assisting Council in providing a service to the community.

Accountability

The *Information Privacy Act 2009 (Qld) (IP Act)* does not impose a mandatory obligation on Queensland government agencies to notify the Office of the Information Commissioner (OIC) or affected individuals in the event of a privacy breach. Regardless, the same principle applies as in the Commonwealth's scheme – that Council should foremost consider the impact of the breach on the victim and take all reasonable steps to minimise any potential damage.

Breach Management and Notification

Council will consider the following factors when responding to a privacy (or suspected) breach:-

1. breach containment and preliminary assessment;
2. evaluation of the risks associated with the breach;
3. notification (if applicable) ; and
4. prevention.

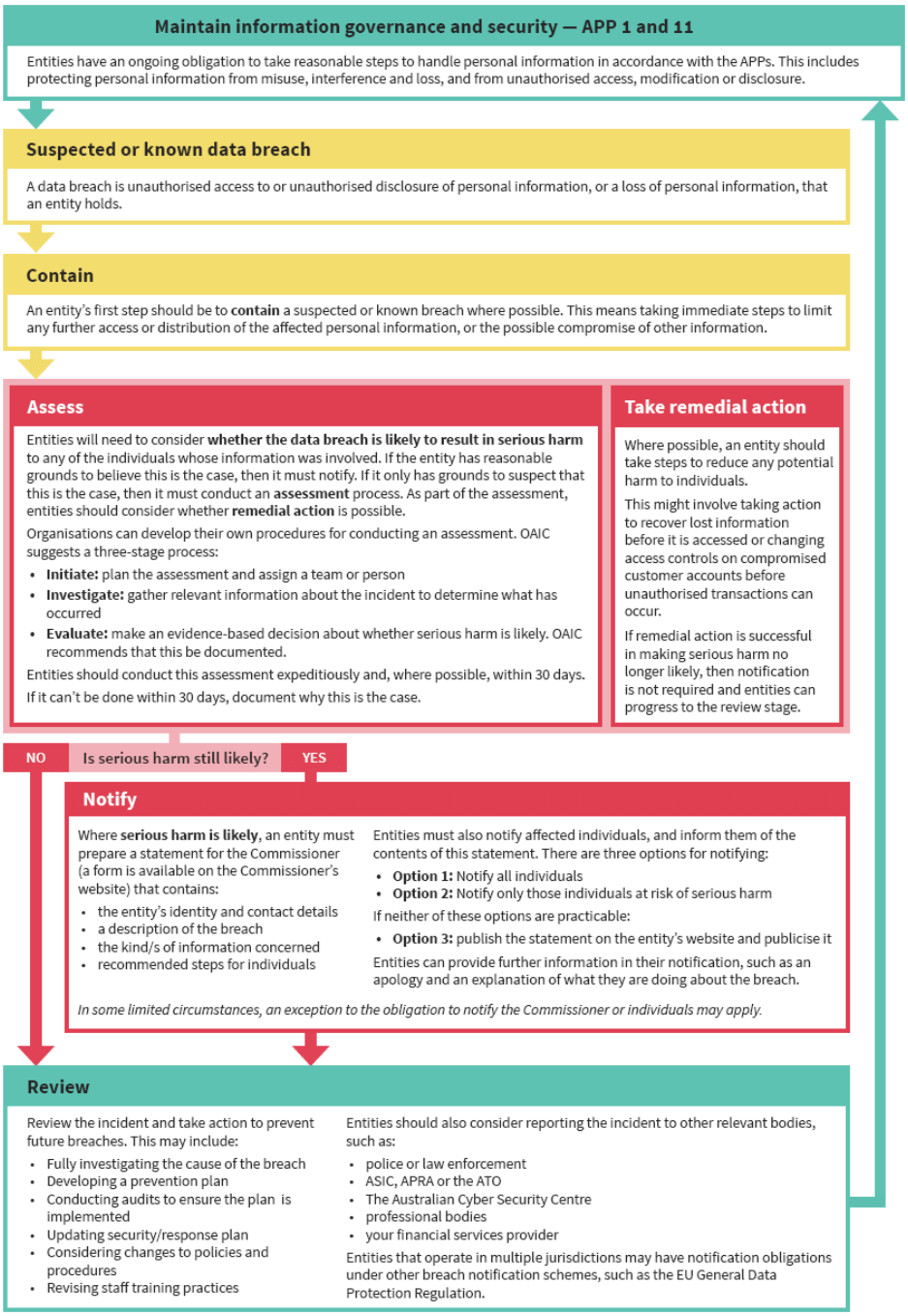
Decisions on a response to a privacy breach will be done on a case by case basis by a sufficiently senior authorised officer, being the Manager of the relevant Department where the breach occurred. The Responsible Manager, under the general direction of their relevant General Manager and/or Chief Executive Officer, may form an Incident Response Team. The breach containment and preliminary assessment, evaluation of risk associated with the breach and notification (if applicable), will be implemented as soon as possible. The prevention stage is considered a longer term measure, intended to assist with future prevention and early detection strategies.

Data breaches involving tax file number information are also subject to the Notifiable Data Breaches scheme.

Western Downs Health Services Subject to the *Privacy Act 1988* (Cwth)

Western Downs Health Services (ie. Aged Care, Home and Community Care) as health service providers are subject to the Commonwealth's *Privacy Act 1988* and Australian Privacy Principles (APPs) contained therein. Further, Council's health service providers must comply with Notifiable Data Breaches (NDB) scheme which provides requirements for entities in responding to data breaches, providing breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

The following provides an overview of a typical data breach response, including the requirements of the NDB scheme. Officers should refer to the *Data breach notification - A guide to handling personal information security breaches* and the *Guide to developing a data breach response plan* available on the Office of the Australian Information Commissioner's website in the event of a data breach or suspected breach involving Council's health services providers:-



Document Set ID: 1205112
Version: 7, Version Date: 12/04/2018

Complaints

In the event that an individual is not satisfied with the manner by which Council has handled their personal information, they may lodge a formal complaint under Council's Complaints Management Process.

DEFINITIONS:

Access – providing an individual with personal information about themselves that is held by Council. This may include allowing that individual to inspect personal information or to obtain a copy of the personal information.

Collection – gathering, acquiring, or obtaining personal information from any source and by any means, including information that Council has obtained by accident or has not requested.

Collection notice - is a written and/or verbal notice advising a person:-

- why the information is being collected;
- details of any law that allows or requires the collection of personal information;
- details of any person or body to whom Council usually gives the information; and
- if any person or body to whom Council regularly gives information in return regularly gives it to any other person or body and Council is aware of this, details of the other person or body.

Consent – voluntary agreement to some act, practice or purpose.

Council officer - includes employees, contractors, volunteers and all others, past and present, who perform work on behalf of Council.

Disclosure – the release of personal information to persons or organisations outside of Council, including the placing of information on Council's website. This does not include giving individuals personal information about themselves.

Personal information – as defined in the IP Act *'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 a natural living person whose identity is apparent, or can reasonably be ascertained, from the information or opinion'*, and includes a photograph or other pictorial representation of a person, but does not include information that is in:-

- generally available publications;
- material kept in public records and archives such as Commonwealth and State archives; or
- anything kept in a library, art gallery, museum for the purpose of reference, study of exhibition.

An **individual** is a natural living person. Information about a company or someone deceased is not regarded as personal information.

Privacy breach – means when personal information is not handled, whether by accident or otherwise, in accordance with the privacy principles.

Sensitive information – means information or an opinion that may give rise to discriminatory practices based on an individual's:-

- racial or ethnic origin;
- political opinions;
- membership of a political association, a professional or trade association or a trade union;
- religious beliefs and affirmations;
- philosophical beliefs;
- sexual preferences or practices;
- criminal records; or
- health.

Document Set ID: 1205112
Version: 7, Version Date: 12/04/2018

Use – the handling of personal information within Council including the inclusion of personal information in a publication.