

# INFORMATION PRIVACY PLAN

## Introduction

Scenic Rim Regional Council has a firm commitment to protecting an individual's right to privacy through the responsible handling of personal information.

The *Information Privacy Act 2009* (Qld) (the Act) provides for access and amendment rights for personal information held by Council. Obligations about the collection, storage, use and disclosure of personal information are provided in the Information Privacy Principles (Principles) included in the Act. The 11 Principles are contained in Schedule 3 in the Act and appear in Appendix "A".

Under the Act, personal information held by Queensland government agencies must be responsibly and transparently collected and managed (including the transfer of personal information held by Council to other agencies, other levels of Government and to the community sector or private sector) in accordance with the Principles.

The Act also provides for a complaints mechanism for any act or practice that is a breach of the Principles.

The aim of this plan is to both assist and assure members of the public and staff in understanding how their personal information is managed within Council and in accordance with the Act. It is also designed to meet Information Privacy Principle 5 (IPP5), which places an obligation on agencies to take steps to ensure that people are aware of the types of personal information held by an agency, why they are held, and how an individual can access their personal information.

This privacy plan incorporates:

- The meaning of personal information;
- The responsibilities of the Mayor, Councillors and Council staff;
- The responsibilities of contractors and consultants to Council; and joint venture partners;
- The types of personal information held by Council;
- The main purposes for which personal information is used;
- How individuals can access personal information held by this office; and
- How individuals can lodge a privacy complaint.

## Personal Information

### **What is personal information?**

Personal information extends to any information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The information does not have to explicitly identify a person. It need only provide sufficient information to lead to the identification of a person. It covers information held in paper or electronic records, including images and sounds.

---

Personal information is not limited to information that is sensitive or confidential, although the degree of sensitivity or confidentiality may influence the way in which the Principles are applied in particular circumstances. Many of the Principles require that reasonable actions be taken, having regard to the specific circumstances and the nature of the information. As such, procedures may vary with the sensitivity of the information.

### **What is not personal information?**

The Principles do not apply to publications that are generally available. Generally available publications include documents such as Council's land records, white pages, electoral rolls, annual reports and the Queensland Government Gazette.

## **Documents**

If a document contains the following personal information the Principles **do not** apply to the information in that document:

### **Covert activity**

- Personal information about an individual arising out of or in connection with a controlled operation or controlled activity within the meaning of the *Police Powers and Responsibilities Act 2000* or the *Crime & Corruption Act 2001*;
- Personal information about an individual arising out of or in connection with a covert undertaking of an operation, investigation or function of a law-enforcement agency; or
- Personal information about an individual arising out of a warrant issued under the *Telecommunications (Interception & Access) Act 1979* of the Commonwealth.

### **Witness protection**

Personal information about a witness who is included in a program under the *Witness Protection Act 2000*, or who is subject to other witness protection arrangements made under an Act.

### **Disciplinary actions and misconduct**

- Personal information about an individual arising out of a complaint made under Part 7 of the *Police Service Administration Act 1990*; or
- Personal information about an individual arising out of an investigation of misconduct or official misconduct under the *Crime & Corruption Act 2001*.

### **Public Interest Disclosure (Whistleblowers)**

Personal information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosure Act 2010*, or that has been collected in the course of an investigation arising out of a public interest disclosure.

### **Other**

Additionally, the Principles do not apply where the:

- Authority to collect, use, store and disclose personal information has an overriding statutory base;
- Personal information is that of a deceased person; or
- Personal information is in a generally available document.

## **Application of this Plan**

Scenic Rim Regional Council's Privacy Plan applies to:

- Mayor, Councillors and Council employees;
- Contractors and consultants to Council; and
- Joint venture partners in projects with Council.

### **Mayor, Councillors and Council Employees**

When dealing with personal information, the Mayor, Councillors and Council employees will comply with the Principles outlined in this Plan.

### **Contractors and Consultants to Council**

Council regularly enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on behalf of Council.

The Act requires personal information to be managed in accordance with the Principles and in regard to any outsourcing arrangements, contracts and licences entered into after 1 July 2010 Council will take all reasonable steps to ensure contractors agree to comply with these Principles.

### **Joint Venture Partners**

Where Council has partnership agreements with companies or individuals, Council will also take all reasonable steps to bind the companies or individuals to comply with the Principles when entering into a new contract or renewal.

### **Responsibilities for Privacy within Council**

The overall responsibility for privacy in Council rests with the Chief Executive Officer. The Mayor, Councillors and all staff have a responsibility to ensure they comply with the Act.

The day to day management of privacy is managed by the Governance Section. The Governance Section is the first point of contact for members of the public and the Mayor, Councillors and employees on privacy matters, including:

- Breach of privacy complaints
- Requests for internal reviews
- Requests to amend records, and
- General information on privacy in Council.

The Governance Section can be contacted at [mail@scenicrim.qld.gov.au](mailto:mail@scenicrim.qld.gov.au) or by phone on (07) 55405111.

The Governance Section is also responsible for reporting privacy matters to the Chief Executive Officer and for preparing relevant statistical reports for senior management.

## **Types of personal information held**

The types of personal information held by Council includes, but is not limited to:

- contact details such as names, addresses, telephone numbers, email addresses;
- personal opinions;
- employee identification;
- information surrounding complaints and grievances;
- gender;
- date of birth;

- bank account details;
- pensioner and/or concession details;
- electronic transactions;
- internet and intranet activity;
- transaction history;
- relevant details applicable to processing various applications;
- details required and associated information kept in the investigation of complaints and requests for action;
- images and recordings;
- CCTV imagery for public safety purposes;
- details of receipts and payments;
- land record information; and
- survey responses and submissions.

## **Main purposes for which personal information is used**

Council holds electronic and paper records containing personal information, which can broadly be divided into two classes:

1. Records relating to staff employment and corporate support; and
2. Records relating to the performance of Council's business and service delivery functions.

### **1. Records relating to staff employment and corporate support**

#### **Employee Records**

These documents are used to manage employment matters effectively and relate to all current and former employees (permanent, contract and temporary) and applicants for vacant positions. Appropriate security measures are in place for this information, appropriate to the sensitivity of personal information it contains. These documents include:

- attendance and overtime records;
- medical matters;
- tax file number declaration forms;
- personal history files;
- recruitment matters;
- character checks and security clearances;
- performance appraisals, including recommendations for honours and awards;
- trade, skill and aptitude tests;
- work related travel;
- contracts and conditions of employment;
- leave applications and approvals;
- payroll and pay, including banking details;
- declarations of pecuniary interests;
- education, personal development and training;
- contracts and conditions of employment;
- disciplinary and counselling matters, including complaints, grievances, investigations and associated actions;
- allegations and investigations of alleged misconduct;
- personal history and welfare matters;
- accidents and injuries, including compensation and rehabilitation case files;
- electronic transaction history including telephone activity, emails, internet and intranet activity, security pass activity;
- next of kin details;
- workplace health and safety matters;

- Council fleet management; and
- other staff and establishment records as appropriate.

### **Financial Management Records**

The purpose of these records is to process and account for Council's revenue and expenditure in the conduct of its business and service delivery. The records include personal information of ratepayers, creditors, debtors, outsourced services and service providers.

### **Information Services Records**

Council's information management systems routinely contain much of the core business and the supporting corporate services of Council on behalf of its many functional areas. This encompasses a wide variety of electronic transactions. Records within this networked environment will generally cover information referred to in other parts of this plan that deal with the core business operations of functional areas of Council. The use of these systems is routinely monitored by internal and external control systems.

## **2. Records relating to the performance of Council's business and service delivery functions**

### **General Information**

These documents assist Council in the effective and efficient operation of Scenic Rim Regional Council. Relevant documents include messages, inwards and outwards correspondence, transaction history, registers, minutes, lists and directories.

### **Land Records**

Council holds personal information relating to each parcel of land. This information includes ownership details, contact details, transaction history and property history. This information is used to provide efficient and effective services, levy appropriate rates and meet legislative requirements.

### **Application Details**

Council holds personal information for processing applications, permits, licences or approvals for which Council is responsible. The personal information includes contact details and any other information that is relevant to the processing of the application. This is to ensure that Council makes decisions in accordance with applicable protocol, legislation and service requirements. This collection of personal information extends to all avenues where Council is responsible for administering and processing applications, including:

- Town planning applications;
- Operational works applications;
- Building and plumbing applications;
- Health and environment licences and approvals;
- Animal management services;
- Cemetery applications;
- Requests relating to rating matters;
- Property access and rural road numbering applications;
- Road infrastructure permits and approvals;
- Grant applications;
- Immunisation requests;
- Land record applications and search requests; and
- Applications to carry out works or supply goods for Council.

### **DAP Online**

Personal information may also be contained in development applications submitted to Council. Properly made applications are published on Council's Planning and Development Online service (DAP Online) per section 736 of the *Sustainable Planning Act 2009* (the Act).

### **Requests for Action - General Services**

Council receives personal information from customers requesting actions from Council, and this information is used to enable Council to effectively deliver a service to that customer. This includes contact details and telephone conversation records of customers requesting related Council related services including, but not limited to:

- Council's road network;
- Network infrastructure delivery
- Council controlled parks, gardens, cemeteries and reserves;
- Roadside landscaping;
- Waste management services;
- Pest management services;
- Rural road numbering;
- Stormwater and drainage issues; and
- Council owned buildings.

### **Requests for Action and Investigations of Complaints - Regulatory Services**

Council also receives grievances from the general public that require action under statutory instruments, including applicable investigation. The personal information held includes contact details and telephone conversation records of the complainants, and also personal information relating to the subject of the complaint relevant to the investigation of the matter. Generally, these matters relate to:

- Council issued licences, permits and approvals;
- Declared pest management issues on private land;
- Animal management;
- Environmental pollution and public health matters;
- Building, plumbing and swimming pools; and
- Development compliance matters.

### **Community Services**

In addition to the services mentioned above, Council also holds personal information that is required for the effective and efficient delivery of the following services:

- Customer Service
- Library services;
- Management, maintenance and access to Council owned facilities (including swimming pools, buildings, parks, gardens and reserves);
- Management, maintenance and access to Council keys;
- Management and maintenance of Council controlled cemeteries;
- Community engagement functions;
- Emergency services management;
- Corporate governance management;
- Environmental activities such as workshops, events, programs (eg. land for wildlife, conservation covenant, rural trees, compost bin rebates);
- Membership database for community groups and conservation groups;
- Regional development activities such as workshops and economic development activities;
- Cultural services activities including event bookings and display of artwork; and
- Community development activities including grant applications and visitor information centres.

While every effort has been made to include an extensive list of the types of personal information held by Council, and the purposes for which they are used, Council may hold other types of personal information than the examples provided.

### **Public registers managed within Council**

Public registers will be identified from time to time and their maintenance and use incorporated within Council's personal information management practices. Where authorised by law, these registers appear on Council's website.

### **Expression of Interest and Tenders**

Expression of Interest and Tender documents submitted to Council may also contain personal information and is dealt with in accordance with the *Information Privacy Act 2009*.

## **Retention and Disposal of Records**

The disposal of Council's records is governed by the *Public Records Act 2002*, which governs the making and preservation of public records in Queensland. Council retains records in accordance with this legislation, the *Queensland State Archives General Retention and Disposal Schedule for Administrative Records*, and the *Local Government Sector Retention and Disposal Schedule* approved by Queensland State Archives. All disposals must go through an appropriate approval process, and the disposal is carried out in a secure manner.

## **Access and Amendment Procedures**

Under the Act, there are controls on how personal information is managed. The rights of access and amendment are dealt with under Chapter 3 of the Act. Those rights are confined to the person to whom the personal information directly and personally relates and to their children under 18 years of age.

Information Privacy Principle 6 provides that a person is entitled to access any record that contains their personal information except where access is restricted by any law.

Information Privacy Principle 7 provides that a person is entitled to seek an amendment of any record that contains their personal information that is misleading, irrelevant, not up-to-date or incomplete.

Persons wishing to access their personal information held by Council or to amend that information may submit an informal request to Council at:

Mail: PO Box 25, Beaudesert Qld 4285

Fax: 07 5540 5103

Email: [mail@scenicrim.qld.gov.au](mailto:mail@scenicrim.qld.gov.au)

Phone enquiries: 55405111

Any person who is dissatisfied with the outcome of their informal request to access or amend their personal information may submit a formal application to Council using the prescribed form:

[Right to Information and Information Privacy Access Application Form](#)

[Information Privacy Personal Information Amendment Application Form](#)

## **Complaint and Review Process**

If an individual believes that the Council has not dealt with their personal information in accordance with the Act, they may make a complaint to the Council.

Council must respond to complaints within 45 business days of receipt. If the complainant has lodged a formal written complaint and does not agree with the response they may refer a written complaint to the Office of the Information Commissioner. The complainant cannot make a written complaint to the Office of the Information Commissioner until they have given Council 45 business days to respond to their complaint.

Complaints or enquiries should be directed to the address above where they will be forwarded to the Governance Section.

If you would like complaint handling documents sent to you, more information on the complaints process or on privacy matters in general, please contact the Governance Section on the contact details above.

**Approved by:**

**Jon Gibbons**  
**Chief Executive Officer**  
**18 January 2018**

**Privacy Plan Document Details:**

File Reference Number: 17/08/003  
Contact Officer: Coordinator Governance and Corporate Policy  
Next Review Date: 1 September 2019



## Appendix A - Information Privacy Principles

### Information Privacy Principle 1

#### (Collection of personal information [lawful and fair])

- (1) An agency must not collect personal information for inclusion in a document or generally available publication unless -
  - (a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and
  - (b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.
- (2) An agency must not collect personal information in a way that is unfair or unlawful.

### Information Privacy Principle 2

#### (Collection of personal information [requested from individual])

- (1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.
- (2) However, this section applies only if the agency asks the individual the subject of the personal information for either -
  - (a) the personal information; or
  - (b) information of a type that would include the personal information.
- (3) The agency must take all reasonable steps to ensure that the individual is generally aware of:
  - (a) the purpose of the collection; and
  - (b) if the collection of the personal information is authorised or required under a law -
    - (i) the fact that the collection of the information is authorised or required under a law; and
    - (ii) the law authorising or requiring the collection; and
  - (c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the **first entity**)—the identity of the first entity; and
  - (d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the **second entity**)—the identity of the second entity.
- (4) The agency must take the reasonable steps required under subsection (3) -
  - (a) if practicable - before the personal information is collected; or
  - (b) otherwise - as soon as practicable after the personal information is collected.
- (5) However, the agency is not required to act under subsection (3) if -
  - (a) the personal information is collected in the context of the delivery of an emergency service; and  
*Example -*  
Personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service
  - (b) the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and
  - (c) the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

**Information Privacy Principle 3  
(Collection of personal information [relevance etc])**

- (1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.
- (2) However, this section applies to personal information only if the agency asks for the personal information from any person.
- (3) The agency must take all reasonable steps to ensure that -
  - (a) the personal information collected is -
    - (i) relevant to the purpose for which it is collected; and
    - (ii) complete and up to date; and
  - (b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

**Information Privacy Principle 4  
(Storage and security of personal information)**

- (1) An agency having control of a document containing personal information must ensure that -
  - (a) the document is protected against -
    - (i) loss; and
    - (ii) unauthorised access, use, modification or disclosure; and
    - (iii) any other misuse; and
  - (b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.
- (2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

**Information Privacy Principle 5  
(Providing information about documents containing personal information)**

- (1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out—
  - (a) whether the agency has control of any documents containing personal information; and
  - (b) the type of personal information contained in the documents; and
  - (c) the main purposes for which personal information included in the documents is used; and
  - (d) what an individual should do to obtain access to a document containing personal information about the individual.
- (2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

**Information Privacy Principle 6  
(Access to documents containing personal information)**

- (1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.
- (2) An agency is not required to give an individual access to a document under subsection (1) if -
  - (a) the agency is authorised or required under an access law to refuse to give the access to the individual; or
  - (b) the document is expressly excluded from the operation of an access law.

**Information Privacy Principle 7  
(Amendment of documents containing personal information)**

- (1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information -
  - (a) is accurate; and
  - (b) having regard to the purpose for which it was collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.
- (2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.
- (3) Subsection (4) applies if -
  - (a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and
  - (b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).
- (4) The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

**Information Privacy Principle 8  
(Checking of accuracy etc. of personal information before use by agency)**

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, complete and up to date.

**Information Privacy Principle 9  
(Use of personal information only for relevant purpose)**

- (1) This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.
- (2) The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

## Information Privacy Principle 10 (Limits on use of personal information)

- (1) An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless -
- (a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the other purpose; or
  - (b) the agency is satisfied on reasonable grounds that use of the information for the other purpose 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 the information for the other purpose is authorised or required under a law; or
  - (d) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for 1 or more of the following by or for a law enforcement agency -
    - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or 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; or
  - (e) the other purpose is directly related to the purpose for which the information was obtained; or
 

*Examples for paragraph (e) -*

    - 1 An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.
    - 2 An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivering improvements to the core services.
  - (f) all of the following apply -
    - (i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest;
    - (ii) the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information;
    - (iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.
- (2) If the agency uses the personal information under subsection (1)(d), the agency must include with the document a note of the use.

## Information Privacy Principle 11 (Limits on disclosure)

- (1) An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the **relevant entity**), other than the individual the subject of the personal information, unless -
- (a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or
  - (b) the individual has expressly or impliedly agreed to the disclosure; or

- (c) the agency is satisfied on reasonable grounds that the disclosure 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) the disclosure is authorised or required under a law; or
  - (e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency -
    - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or 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; or
  - (f) all of the following apply -
    - (i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
    - (ii) the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;
    - (iii) it is not practicable to obtain the express or implied agreement of the individual before the disclosure;
    - (iv) the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.
- (2) If the agency discloses the personal information under subsection (1)(e), the agency must include with the document a note of the disclosure.
- (3) If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not use or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.
- (4) The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that -
- (a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and
  - (b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and
  - (c) the individual has not made a request mentioned in paragraph (b); and
  - (d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and
  - (e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically.