

ORGANISATIONAL POLICY

PRIVACY POLICY

Corporate Plan Reference:	8. Great Governance 8.1 Ethical, accountable and transparent decision making 8.1.1 Develop and implement a governance framework that provides transparent and accountable processes and enhances council's reputation 8.1.2 Ensure legislative compliance and awareness
Endorsed by Chief Executive Officer:	John Knaggs 1 July 2010
Policy Owner and Department:	Kim Driver, Organisation Performance

INTRODUCTION

The Queensland Information Privacy Act was introduced in July 2009. It forms part of a new information regime. It is applicable to Local Governments from 1 July 2010.

Information Privacy is about protecting the personal information of individuals in accordance with the Information Privacy Act 2009 (the Act). The Act provides for access and amendment rights for personal information held by Sunshine Coast Regional Council (Council).

Obligations about the collection, storage, security, access, amendment and use and disclosure of personal information are provided in the 11 Information Privacy Principles included in the Act.

Personal information is defined in the Act as information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Examples of the types of information collected, and its use and disclosure, are given at **Appendix A**.

POLICY PURPOSE

This policy articulates the framework for the use and disclosure, quality and security, and access and correction of personal information at the Sunshine Coast Regional Council.

POLICY OUTCOME

It is intended that the outcomes of this policy are:

- Compliance with the Act and the 11 Information Privacy Principles (IPP's).
- Awareness by members of the public of how personal information is managed within Council and how they can seek assurance that their personal information is maintained in accordance with the Information Privacy Act 2009.

- Education of employees who deal with personal information and provide a strategic overview for achieving compliance by Sunshine Coast Council with the Information Privacy Act 2009 and the 11 privacy principles.
- Contributing to the achievement of great governance.

POLICY SCOPE

This policy applies to all personal information collected, used and stored by Council in every aspect of its operations and performance.

This policy applies to all Councillors, council employees, volunteers, contractors, consultants and joint venture partners.

In accordance with the Act, the 11 IPP's do not apply to:

- Personal information about an individual arising out of an investigation of misconduct or official misconduct under the Crimes and Misconduct Act 2001.
- Personal information about an individual that is contained in a public interest disclosure within the meaning of the Whistleblowers Protection Act 1994, or that has been collected in the course of an investigation arising out of a public interest disclosure.
- Personal information where the authority to collect, use, store and disclose personal information has an overriding statutory base and where the personal information concerns a deceased person.
- Personal information does not include information contained in publications that are generally available. Generally available publications include, for example, magazines, books, a newsletter, or a newspaper article, annual reports and the Queensland Government Gazette.

POLICY STATEMENT

The Sunshine Coast Regional Council is committed to protecting the personal information about individuals consistent with the Act and the 11 IPP's.

GUIDING PRINCIPLES

The principles that guide the application of this policy are:

- Council will collect, use and store personal information in accordance with the Information Privacy Act 2009
- Council will inform itself, its staff and its community about protecting personal information
- Council will apply the 11 Privacy Principles as an integral part of its business processes.
- All Councillors, council employees, volunteers, contractors, consultants and joint venture partners are bound by the principles of the Information Privacy Act 2009.

INFORMATION PRIVACY PRINCIPLES

The Act sets out 11 IPP's and these are listed at **Appendix B**. The 11 privacy principles can be grouped into four categories and their application at Council is described below.

Collection

Council will only collect personal information that is directly related to the functions and services provided by Council. Where possible, Council will advise what the information will be used for either prior to or at the point of collection.

Storage and Security

Council will make every effort to ensure that the personal information it collects, uses and stores is relevant and to the extent necessary, accurate, complete and up-to-date for the purpose for which it is to be used.

Council will endeavour to maintain a secure system for storing personal information and will utilise appropriate technologies, security methods, operational policies and procedures to protect the information from unauthorised access, improper use, alteration, unlawful or accidental destruction and accidental loss.

All personal information will be removed from Council systems where it is no longer required for any purpose.

Access and Amendment

Individuals may have access to their personal information and may seek to have this information corrected.

Written applications for access and correction will be (handled) by Council. Applications will be (handled) in accordance with the provisions of the Act.

Use and Disclosure

Council will use personal information it collects for the primary purpose for which it was collected. Additionally, Council may use the information for other (identified/ non identified) purposes where the individual has consented to the use or disclosure.

COMPLAINTS

An individual may lodge a complaint with the Manager Corporate Governance regarding the handling of personal information.

Alternatively, individuals may lodge a complaint with the Information Privacy Commissioner.

IMPLEMENTATION

This policy is supported by the Act, fact sheets from the Information Privacy Commissioner, the Information Privacy page on Council's intranet and information on Council's website.

ROLES AND RESPONSIBILITIES

All Council employees have access to personal information subject to security authorisation clearance and operational need; and employees are routinely reminded of system usage rules and monitoring procedures concerning the collection and use of the information. Additionally, all Council employees are bound by the Local Government Act 2009, Public Sector Ethics Act 1994 and, specifically the five ethics principles and the Employee Code of Conduct. In this context, all employees have a responsibility to comply with the Information Privacy Act 2009 and the 11 Information Privacy Principles in the course of undertaking their duties.

DEFINITIONS

Personal information - *Personal information is an opinion or information, whether true or false, that identifies or could identify an individual. It does not have to be written down – it could be spoken information, information in a database or on a computer screen, or a photograph or video recording. Examples of personal information are:*

- *date and place of birth*
- *religious or political beliefs*
- *financial, criminal or medical records*
- *family arrangements*
- *street address, telephone number and email address*
- *where a person works or goes to school.*

Depending on the type of information and the context, the information or opinion does not have to include the name of an individual to be personal information¹.

Information Privacy Principles - *11 privacy principles that set out how Queensland government agencies should collect, use, store, secure, and disclose personal information.*

RELATED POLICIES AND LEGISLATION

Privacy Act 1988 (Commonwealth)
 National Privacy Principles (Commonwealth)
 SCRC Code of Conduct
 Fraud & Corruption prevention
 Local Government Act 2009 and regulations
 Right to Information Act 2009
 Public Sector Ethics Act 1994

Version control:

Version	Reason/ Trigger	Change (Y/N)	Endorsed/ Reviewed by	Date
1.0	Eg. Create new			DD/MM/YYYY
	Eg. Review			

¹ [Office of the Information Commissioner, Information Sheet “Your Privacy Rights”](#)
 Sunshine Coast Council



CLASSES OF PERSONAL INFORMATION HELD

Introduction

Sunshine Coast Council (Council) collects, stores, uses and in certain instances discloses personal information as both an employer and service provider to the community.

Depending on the purposes for the collection of personal information, personal information may be retained in Council's record management system, payroll system, financial management system, electronic databases and PD Online. Some portions of this information may be retained in various business units while being used for specific purposes.

In all cases personal information is retained in accordance with the *Public Records Act 2002* and *regulation* and according to the categories set out in the general retention and disposal schedule issued by Queensland State Archives. Records may be stored on both paper and electronic media.

This document provides examples of where Council may collect, use, store and disclose personal information. The details contained in this document are not an exhaustive list and serves only as a guide.

COMMUNITY

Council collects stores and uses personal information to administer and provide services, provide access to library and information technology services. This information is used to administer rates notices, licences; permits, infringements e.g. dogs licences, food licences, public open space permits etc.

Closed Circuit Television (CCTV) photographic imagery may be taken in the act of providing employee and public safety and in the interest of protecting Council assets. CCTV photographic imagery will be retained only in electronic form and is only accessed by an authorised officer responsible for the maintenance and security of Council.

Personal information contained in these records may include:

- Name
- Address
- Phone Number
- Residential status
- Car Registration Number
- CCTV photographic imagery

As an example, only portions of the information held in Council records is disclosed outside the Council to

- The Australian Taxation Office
- Insurance brokers

- Collection agencies
- Personal financial institutions
- Department of Immigration and Citizenship
- Overseas and Australian sponsorship agencies

EMPLOYEES AND RECRUITMENT

Council collects stores and uses employee personal information to administer employment, recruitment, workforce planning, training and payroll and maintain historical employment and payroll records. Some of this information may also be used to administer access to library and information technology services.

As an example personal information contained in these records may include:

- records relating to attendance and overtime
- leave applications and approvals
- medical records
- payroll and pay related records including banking details
- tax file numbers declaration forms
- personal history files
- performance appraisals
- records relating to personal development and training
- graduate, volunteer and work experience scheme participation
- qualifications or licences
- CCTV Photographic imagery retained for employee and public safety

Only portions of the information held in Council employee records are disclosed outside the Council, for example:

- the Australian Taxation Office
- superannuation providers
- compensation providers
- the staff members financial institution

VENDORS/CONTRACTORS

Sunshine Coast Regional Council collects stores and uses vendors' personal or business information to administer the purchasing of goods and services and to administer the tendering process.

Personal information contained in these records may include:

- Contact details of vendors and where volunteered of nominated officers or staff
- records relating to tenders, ordering, invoicing and payment and related records including banking details
- records relating to complaints and investigations

Information held in Council records is normally disclosed outside the Council to the vendor's financial institution.

TENANCY AND SHORT TERM HIRING OF COUNCIL PREMISES

Sunshine Coast Regional Council collects stores and uses business operator's personal or business information to administer the tenancy of business premises on its owned and/or controlled land, to administer the short term hiring training and conference facilities on Council owned and/or controlled property.

Personal information contained in these records might include:

- Contact details of tenant business's principals, and where volunteered, of other nominated officers or employees
- Contact details of hirers, and where volunteered, of other nominated officers or employees
- Records relating to requests for tenancy, to hire, or to reside, invoicing and payment and related records including banking details
- Records relating to complaints and investigations

Only portions of the information held in Council records are disclosed outside the Council to the hirer's or tenants financial institution, and in the event of arrears of payment, to a debt collection agency.

INFORMATION SERVICES CLIENTS

Council collects stores and uses personal information about clients who may not be employees of Council in order to administer access to library and information technology services. The type of personal information held in these records includes:

- name, contact address and details
- records relating to requests for library and information technology access and approval
- records relating to replacement costs for lost library items
- records relating to complaints and investigations

CONTRACTS, JOINT VENTURES AND PARTNERSHIP ARRANGEMENTS

Council collects stores and uses personal information about council officers and the community of various organisations in order to administer contracts and partnership arrangements. For some of these arrangements this information is also used to administer services etc. The types of personal information contained in these records include:

- Contact details of organisations and where volunteered of nominated officers or employees;
- records relating to contracts, tenders, ordering, invoicing and payment and related records including banking details;
- records relating to contract performance, complaints and investigations

There are no requirements to disclose this information outside the Council except where required by law.

ENFORCEMENT NOTICES

Council collects stores and uses personal information to administer the issuing of parking permits, the collection and issuing of penalty enforcement notices (PINS) and to process vehicle infringement notices received from outside organisations in relation to Council vehicles. The type of personal information contained in these records may include names and addresses, driver's licence number, vehicle details, records relating to requesting and approving parking permits, and records relating to PINS.

Some portions of this information are shared with payroll who administer employee payments for PINS, and cashiers for referencing when receiving PINS payments. Information relating to unpaid PINS is also provided to and held by the State Penalties Enforcement Registry (SPER).

Portions of this information relating to unpaid PINS are disclosed outside the Council to SPER in accordance with the State Penalties Enforcement Act 1999 and regulations. Information relating to any Council vehicle infringement notice is disclosed outside the Council to the organisation issuing the infringement notice e.g. Queensland Police Service.

INSURANCE

Council collects stores and uses personal information in order to secure insurance cover in relation to Council activity and also to assist in the settlement of insurance claims. These claims include but are not limited to personal property, vehicle comprehensive insurance, corporate travel and workers compensation insurance. Personal information is collected based on the requirements of the insurance company involved and may include medical history and financial information.

The information held in Council records is disclosed outside the Council to the Council's insurers and insurance brokers.

INFORMATION TECHNOLOGY MANAGEMENT SYSTEMS

The Council's information technology management systems network routinely carries, enables processing of, and stores for varying periods, much of the core business and the supporting corporate service business of the Council on behalf of its many business Units.

Personal information contained in these records might include:

- Names of elected officials and their contact details
- Names of employees and their contact details
- Content of emails as well as email aliases both Council, and if supplied, ones of a private nature
- Details of web sites visited while using the Council's internet
- Details of phone numbers called
- Files and information created on the Council's servers
- Records relating to requests for information technology access, and problems relating to such access
- Summaries of information such as status and nature of employment as required in order to administer information technology access

This information is not usually disclosed except to managers, systems administrators and the person concerned.

RIGHT TO INFORMATION

Personal information is collected when the Council receives a Right to Information request to access, amend and obtain information. Some of the documents gathered to process the request may contain personal information.

Access is limited to the Right to Information Officer and the Manager Corporate Governance, and to the person to whom the records relate or an appropriate nominee.

This information may be disclosed outside the Council to the Information Commissioner in the case of an external review of an RTI decision.

INTERNAL AUDIT

The Council's Internal Audit Unit may collect personal information during the conduct of audits performed in accordance with the International Standards for the Professional Practice of Internal Auditing as pronounced by the Institute of Internal Auditors. For instance, payroll reports and leave forms.

Access is limited to the Chief Executive Officer and Internal Auditors. Information contained in these records may be disclosed outside the Council to an external auditor as required by the Queensland Audit Office.

Schedule 3 Information privacy principles

section 26

1 IPP 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.

2 IPP 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).

3 IPP 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.

4 IPP 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.

5 IPP 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.

6 IPP 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.

7 IPP 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.

8 IPP 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.

9 IPP 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.

10 IPP 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.

11 IPP 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.