CITY OF
MONASH

INFORMATION PRIVACY

POLICIES & PROCEDURES

MAY 2002 & FEBRUARY 2015

Introduction

The Privacy and Data Protection Act 2014 provides for the regulation of the collection, use, security and management of personal information. It also provides for an access and complaints system.

Personal Information

Personal information is information or an opinion about an **individual** whose identity is apparent or can reasonably be ascertained from that information. Such information includes information that forms part of a database.

Policies and Procedures

A number of corporate policies and procedures have been prepared to address the requirements of the Act. These policies and procedures are attached and must be fully adhered to as from 1 September 2002, by all areas of the organisation, in all their activities where personal information is involved.

The policies & procedures address the following –

- Gaining consent to collect and use personal information
- Collection of personal information
- Use & disclosure of personal information
- Security & destruction of personal information
- Accessing & correction of personal information
- Personal information in public registers
- Complaints regarding improper use of personal information

Contractors/third parties

Particular attention should be given to the requirement that any contractor working for Council or a third party involved with Council must adhere to the requirements of the Privacy and Data Protection Act. This is emphasised in the policies & procedures.

Queries/concerns

Any questions or concerns about the policies & procedures should be directed to Council's Information Privacy Officer, phone 9518 3696.

Policy on Gaining Consent to Collect and Use Personal Information

Purpose

Address the requirement to gain a person's consent to have their personal information collected, used and where appropriate/necessary, forwarded to a third party.

Part 1

A person's consent is to be sought unless there are sound, justifiable reasons permitted by the *Information Privacy Act* 2000 and its Information Privacy Principles, *or legislation requires or permits collection.*

Part 2

Criteria for consent

1. Consent must be informed

The person from whom the information is collected must be told what they are consenting to. This means knowing –

- what is being collected, used or disclosed and why;
- who/what organisation is collecting, using or receiving/likely to receive the information; and
- the consequences(if any) if consent is not given

2. Consent must be freely given

There must be no coercion in obtaining the person's consent. If a genuine choice is not offered, the proposed action can only proceed if permitted by legislation.

3. Consent must be specific

Consent is to be sought for the collection or use of specific information, for an identified purpose, by identified people/organisation, for an identified period of time.

4. Consent must be current

Consent must apply to a person's circumstances at the time; it should be able to be revoked.

Part 3

'Express' and 'Implied' Consent

There are two types of consent – 'express' and 'implied'.

- Express consent is unequivocal consent that does not require any inference.
- Implied consent is consent that can only be inferred by the actions of the person from whom the consent is sought.

Where possible/appropriate, express consent must be sought/obtained.

Part 4

Verbal & written consent

Where a person's consent is sought or obtained verbally, detailed file notes should be kept regarding, the name of the person giving consent, the date and time consent was given and whether consent was obtained over the phone or in person.

Where written consent is sought, the request should be easy to find and expressed in clear language.

Part 5

'Opt in' and 'Opt out' Consent

Whether consent is sought in writing or orally, it should be either 'opt in' or 'opt out'.

'Opt in' consent means the Council only takes a course of action if the person concerned gives their consent.

Example 1

Do you consent to the use/disclosure of the information collected in this form by/to ABC company/agency/department for the purpose of XYZ?

Please tick the appropriate box: □YES □NO

Example 2

Please tick the appropriate box –

□ Yes I agree to the use/disclosure of the information collected in this form to ABC for the purpose of XYZ.

□ No I do not agree to the use/disclosure of the information collected in this form to ABC for the purpose of XYZ.

'Opt out' consent means the Council takes a course of action unless the person indicates that they do not consent.

Example

It is our usual practice to use /disclose the information collected in this form to ABC for XYZ purpose.

If you do **not** want us to do this in your case, please tick this box □.

Policy on Collection of Personal Information

Purpose

To govern the collection of personal information by the Council and its representatives, agents, contractors, etc.

Reference must be made to the following Council policies –

'Policy on Gaining Consent to Collect and Use Personal Information'
'Policy on Use of Personal Information'

before any activity involving collection of personal information is undertaken.

PART 1

Compliance with the Act's Information Privacy Principles
In all activities concerning the collection of personal information whether by the Council or its contractors, the following must be strictly adhered to –

1. Personal information must only be collected if it is necessary for one or more of the Council's functions or activities.
2. Collection must only be by lawful and fair means and not in an unreasonable or intrusive way.
3. Before or at the time of collection (or, if that is not possible, as soon as practicable after) of the personal information, reasonable steps must be taken to ensure that the individual is aware of-
   (a) the identity of the organisation and how to contact it;
   (b) the right they have to gain access to the information;
   (c) the purposes for which the information is collected;
   (d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind;
   (e) any law that requires the particular information to be collected; and
   (f) the main consequences (if any) for the individual if all or part of the information is not provided.
4. If it is reasonable and practicable to do so, personal information about an individual must be collected directly from them.
5. If personal information about an individual is collected from someone else, reasonable steps must be taken to ensure that the individual is made aware of the matters listed in 3 (a) to (f) above, except where making them aware would pose a serious threat to their life.

Collection by a third party on the Council's behalf

All third parties collecting information on the Council's behalf, must:

1. Be informed in writing of the *Information Privacy Act* 2000 Information Privacy Principles and the responsibilities thereunder; and
2. Provide a written undertaking to:

   a) comply with the Information Privacy Principles through a confidentiality undertaking.

b) indemnify the Council against any action taken by a person as a result of any action by the contractor which leads to a breach of any provision of the Act.

c) agree that its obligations in respect of its compliance and confidentiality undertakings survive the termination or expiration of the contract.

d) return/give to the Council all personal information records, documents, information, etc, in its possession created or maintained for the purpose of the contract/agreement, upon the completion or termination of the contract/agreement or by the date specified in the contract/agreement.

3. Agree in writing that all information they collect under the contract/agreement remains the property of the Council.

PART 2

Collection procedures – identification, disclosure of purpose of collection & use of information

The following actions must be taken at the time of collection –

Identification: The person collecting the information must identify themselves to the person from whom the information is being collected, by providing their full name and stating that the information is being collected on behalf of the Council.

An employee/representative of a Council contractor, collecting the information must give their name, the organisation they work for and state that the information is being collected for the Council.

Purpose of the collection: The true reason for collecting the personal information must be given, including if there is a legal/statutory requirement for the collection.

Who the information will or may be disclosed to: The person from whom the personal information is collected must be told -

- who the information will or may be disclosed to; and
- which organisations (if any) there is a legal/statutory requirement to disclose the personal information to.

Access to the information: The person from whom the information is being collected must be told that they can access the information they are giving, through the Council's Information Privacy Officer.

Contacting the organisation: The person giving the information must be provided with a contact telephone number for the organisation collecting the information and the name of the person in that organisation responsible for the management of the information.

Where an organisation is collecting information for the Council, the names and contact numbers of the responsible individuals for that organisation and for the Council must be provided.

Part 3

Anonymity

Where it is feasible and lawful, individuals are to be given the option of remaining anonymous in their transactions with the Council.

Unique Identifiers

Unique identifiers belonging to another organisation (eg tax file numbers, social security identification numbers, driver's licence numbers, etc) must not be used or adopted by the Council or any of its contractors, agents or representatives unless required by law.

Policy on Use & Disclosure of Personal Information

Purpose

To regulate use and disclosure of personal information by the Council and its contractors, agents, etc.

Reference must be made to the following Council policies prior to any activity relating to the use or disclosure of personal information being undertaken –

'Policy on Gaining Consent to Collect and Use Personal Information'
'Policy on Collection of Personal Information'
'Policy on Security & Destruction of Personal Information'

Use and Disclosure of Personal Information

Personal information must only be used and disclosed for legitimate Council-related activities & for the primary purpose for which it was collected or for a secondary purpose the person may reasonably expect. Use or disclosure for any other purpose must have the consent from the person concerned.

Consent to the use of personal information by a third party

Where the Council intends to forward an individual's personal information to a third party, at the time of collection of the information -

- the consent of that individual to have that information passed on will be sought;
- the identity of the third party will be made known to the individual; and
- the reason for intending to give the personal information to the third party will be made known to the individual.

The information will not be provided to the third party until the consent has been obtained/received.

Personal information will not be provided to a third party, where consent has been refused, unless there is a legal requirement to do so.

Undertakings of confidentiality by a third party

Where information is to be disclosed to a third party, the third party must, in writing -

a) agree to comply with the Information Privacy Principles through entering into a confidentiality agreement with the Council.
b) indemnify the Council against any action taken by a person as a result of a breach of the Act by the third party.
c) agree to its obligations in respect of its compliance and confidentiality undertakings surviving the termination or expiration of the contract/agreement with the Council

prior to the information being disclosed.

NB: Council officers can obtain a template confidentiality agreement from the Council's Information Privacy Officer.

Legal requirement to pass on information

If the Council has a statutory/legal obligation to forward personal information to a third party, the person concerned will be this at the time of the collection and told who the third party is.

Policy on Security & Destruction of Personal Information

Purpose

To require the security of personal information and the use of appropriate procedures for the destruction of outdated personal information.

Part 1

Security of personal information

Personal information must be secured to prevent unauthorised access, removal, interference, loss or alteration.

Access

Access to personal information must only be provided to -

- Council officers or employees with a legitimate reason for accessing the personal information, ie for Council-related activities.
- A third party with legitimate reasons for seeking access in order to fulfil its obligations under a contract or agreement with the Council and that has provided the required written undertakings and indemnities regarding collection, use, security, etc of personal information.
- The Information Privacy Officer, for their investigation of a complaint of breach of privacy, or in the course of responding to a request for access to the personal information.
- State and Commonwealth Government agencies as provided for by legal or statutory requirements.
- The person about whom the information concerns where legislation provides for them to obtain access.

Part 2

'De-identifying' outdated personal information

Outdated personal information must be 'de-identified', ie, remove anything in it that may directly or indirectly assist in or lead to the identification of the individual about whom that information concerns, immediately after the information becomes outdated.

Part 3

Destruction of personal information

Use of 'confidential destruction bins' or some other method guaranteeing confidential and secure destruction of documents and providing documentary evidence of such, must be made for the destruction of outdated personal information.

Before destruction is undertaken, reference should be made to any legal or statutory requirements regarding retention of documents.

Policy on Requests for Access to & Correction of Personal Information

Purpose

To address requests for access to and/or correction of an individual's personal information held by the City of Monash.

PART 1

Where an Information Privacy Principle allows an individual to access or correction of, personal information, that request, or right of access, may be exercised by -

(a) the individual personally, except if the individual is a child who is incapable of making the request; and

(b) an authorised representative of the individual if-

(i) the individual is incapable of making the request or exercising the right of access; and

(ii) the personal information sought is reasonably necessary for the lawful performance of functions, duties or exercise of powers in respect of the individual by the authorised representative.

Definition of 'authorised representative (section 64 of the Information Privacy Act 2000)

An **"authorised representative"**, in relation to an individual, means a person who is-

(a) a guardian of the individual; or

(b) an attorney for the individual under an enduring power of attorney; or

(c) an agent for the individual within the meaning of the **Medical Treatment Act 1988**; or

(d) an administrator or a person responsible within the meaning of the **Guardianship and Administration Act 1986**; or

(e) a parent of an individual, if the individual is a child; or

(f) otherwise empowered under law to perform any functions or duties or exercise powers as an agent of or in the best interests of the individual-

except where acting as an authorised representative of the individual is inconsistent with an order made by a court or tribunal.

PART 2

Processing of request for access to personal information

The Information Privacy Officer will process all requests for access to personal information as follows -

a) only requests received in writing will be processed;

b) the application will be acknowledged & the applicant informed of the decision within 45 days of receipt of the application;

c) the application will be forwarded to the Manager of the relevant area responsible for that information, to –

i) verify the applicant's identity; and

ii) ensure that where the applicant is an 'authorised representative' the necessary authorisation to access the personal material has been submitted; and

iii) locate the personal information & forward it to the Information Privacy Officer

d) the Information Privacy Officer will arrange for access to the personal information by the applicant.

No fee shall apply for access.

Proof of identity

The application must be accompanied by adequate proof of the applicant's identity, eg

- Photocopy of driver's licence
- Letter from solicitor/JP
- Statutory Declaration

Where an 'authorised representative' makes an application, the following will need to accompany that application –

1. Proof of the authorised representative's identity; and
2. Signed written approval from the person about whom the information is about, authorising the applicant to access the information.

Insufficient proof of identity

If the Manager of the area responsible for the personal information requested is not satisfied that adequate proof of identity has been provided, the Information Privacy Officer will write to the applicant within 14 days of receiving the Manager's advice, seeking sufficient proof of identity.

The application will not be processed until proof of identity, which the Manager considers is adequate, has been received.

Denial of access

Denial of a request for access is to be for the reasons detailed in Information Privacy Principle 6 of the *Information Privacy Act* 2000. The Information Privacy Officer will advise the Applicant in writing, within 45 days of receipt of the application, of the decision and the reasons for the denial of access.

Part 3

Requests for Correction or Update of personal information

Requests for correction or updating of personal information must be received in writing and forwarded to the Manager of the relevant area responsible for that information.

The Manager will ensure that the applicant's identity is verified and where the applicant is an 'authorised representative' the necessary authorisation has been submitted.

If the Manager considers that insufficient proof of identity has been provided, they will seek further proof. The application will not be processed until the Applicant has provided adequate proof.

Agreement to correct or update personal information

Where the correction or update is agreed to, the Manager concerned will inform the applicant in writing, within 28 days of receipt of the application.

The correction or update will be made as soon as practicable but no later than 45 days after the date that the request was received.

Refusal to make correction to or to update personal information

If the Manager concerned refuses to make the correction requested they will -

i) notify the Applicant in writing, within 28 days of receipt of the application, advising them that they may then request that a statement be associated with the personal information, claiming that the information is not accurate, complete or up to date; and

ii) advise the Information Privacy Officer, in writing, of the application and the decision to refuse it, within 14 days of the decision having been made.

Part 4

Freedom of Information Act 1982

Appropriate consideration will be given to the requirements of the *Freedom of Information Act* 1982 in any application for access or correction of personal information held by the Council.

Policy on Public Registers

Purpose

To regulate/govern the content of public registers kept/maintained by the Council, in the context of the requirements of the Privacy and Data Protection Act 2014.

Public Registers

Personal information collected, used, held and managed by the City of Monash must be done so in accordance with the Information Privacy Principles.

A public register must not contain personal information unless the legislation under which that register has been created, requires it.

If there is a legal requirement to include personal information in a public register, all reasonable steps must be taken to ensure that access to that information is only provided for legitimate reasons consistent with the legislation relating to that register.

Such reasonable steps includes the requirement that the person seeking access to the register must provide a written reason for seeking access to the personal information, before access is granted.

Access

'Access' is to be defined as viewing/reading the contents of the register only. It is not to be interpreted as permitting the photocopying or electronic scanning of the register unless the legislation, under which the register was established, specifically provides for such copying.

Policy and Procedures Regarding Complaints

Purpose

To establish procedures for the investigation of complaints about Council's use of personal information contrary to the Privacy and Data Protection Act 2014.

Receipt & processing of complaint

1. Complaints must be made in writing and will be treated as confidential.
2. Within 10 days of a complaint being received, the Information Privacy Officer will send the complainant a written acknowledgment.
3. Within 5 days of the complaint being received, the Information Privacy Officer will forward the complaint to the relevant Manager
4. The Manager will provide the Information Privacy Officer with a report on the matter, within 14 days of being notified of the complaint.

Investigation of complaint

The Information Privacy Officer –

1. Will assess the complaint received;
2. Will assess the report from the Manager of the area concerned; and
3. May seek further information from the complainant.

Findings of investigation

Within 14 days of gathering all information he/she deems necessary, the Information Privacy Officer will make a determination on the complaint, having regard to -

1. The Manager's written report.
2. The complaint and any further information obtained from the complainant.
3. Relevant Council procedures and policies.
4. The Privacy and Data Protection Act 2014.

Complaint proven

If the complaint is proven -

1. The Manager of the area concerned will be informed in writing of the finding (copy to Chief Executive Officer) and requested to remedy the breach immediately.
2. Within 14 days of being notified of the finding, the Manager of the area concerned will advise the Information Privacy Officer in writing (with a copy to the Chief Executive Officer), of the action taken to remedy the breach.
3. The Information Privacy Officer will inform the complainant of the result of the investigation & the action to be taken to remedy the breach.

Complaint not proven

If the complaint is not proven –

1. The complainant will be informed of the finding and the reasons for it and that they may make a written request for a review by the CEO within 14 days of receiving notification.
2. The Manager of the area concerned will be informed in writing (with a copy to the Chief Executive Officer) of the results of the investigation.

Request to CEO for a review of finding

Where a complainant makes a written request for a review of the finding -

1. The Information Privacy Officer will acknowledge the request in writing within 10 days of its receipt.
2. The request will be referred to the Chief Executive Officer for determination.
3. The Chief Executive Officer's determination will be forwarded in writing to the complainant, together with advice that should they not be satisfied with the outcome they have 45 days from receipt of the notification to submit a complaint to the Privacy Commissioner.