Greater Dandenong Policy

Privacy & Personal Information Policy

File Number:	A37219	Authority:	Council
Directorate:	Corporate Services	Responsible Officer:	Manager Governance and Commercial Property
Policy Type:	Discretionary	Version No:	004
1st Adopted by Council	9 September 2002 Minute No.	Last Adopted by Council:	10 December 2018 Minute No. 906
Review Period:	Biennial	Next Review:	January 2021

1. Purpose

What has led to the need for this policy?

Greater Dandenong City Council (**Council**) is strongly committed to the transparent and responsible handling of personal and health information and to protecting every individual's right to privacy. Under the *Privacy and Data Protection Act* 2014 and *Health Records Act* 2001 we are bound by the Information Privacy Principles (IPP's) and the Health Privacy Principles (HPP's) outlined in these pieces of legislation.

What will the policy do?

This policy has been developed to meet the requirements of the *Privacy and Data Protection Act* 2014 in regard to the management, collection, use, disclosure and disposal of personal, sensitive and health information and to allow individuals the right to access and, if required, correct information about them which is held by Council or any organisation contracted by Council.

The *Privacy and Data Protection Act* 2014 came into effect on the 17 September 2014 and repealed the *Information Privacy Act* 2000 and the *Commissioner for Law Enforcement Data Security Act* 2005.

Under Part 4 of the *Privacy and Data Protection Act* 2014 (PDP Act) there is a single privacy and data protection framework and a set of standards (known as the Victorian Protective Data Security (VPDS) Standards and Framework) which are intended to strengthen the protection of personal information and other data held by the Victorian public sector. Local government agencies and councils are largely exempt from this part of PDP Act and their essential obligation is to operate in accordance with the Victorian Information Privacy Principles (IPP's) which remain identical in the PDP Act. However, where Council has been appointed as a Committee of Management under s14 of the *Crown Land (Reserves) Act* 1978, it may be subject to the VPDS standards and framework set out in Part 4 of the PDP Act. In this respect, Council will develop protective data security plans in line with the required legislation for the Committees of Management for which it has been appointed and when required to do so.

The Victorian *Health Records Act* 2001 regulates the collection and handling of health information in both public and private sectors due to the likelihood of individuals receiving treatment from both sectors. The *Health Records Act* 2001 establishes 11 Health Principles (HPP's) which apply to the rights of both living and deceased persons.

Council's privacy commitment arises from the need to collect personal and health information to assist in:

- planning and delivering services;
- the follow up and response to concerns and complaints;
- obtaining feedback and monitoring performance;
- requirements to comply under Government legislation; and
- managing employees, contractors, volunteers and stakeholders.

2. Scope

Who does it apply to and what is covered?

This policy applies to:

- all employees, Councillors, contractors, volunteers and stakeholders of the Greater Dandenong City Council.
- all personal, sensitive and health information held by Council, i.e. information or an opinion about an individual whose identity is apparent, or can be reasonably ascertained from that information or opinion. This includes, but is not limited to, information Council has collected in any format including correspondence, in person, over the phone and by electronic means such as the internet.
- personal, sensitive and health information sourced from third parties.

Further, personal information must only be collected and used for the primary purpose for which it was collected, or for a related purpose the person would reasonably expect. For example, where a doctor's certificate informs Council of a person's medical condition, it would be reasonable to expect that the same information might also be used to make reasonable adjustments to support that person's interactions with Council.

This policy is available on Council's website and copies are made available to individuals upon request.

The obligations contained in this policy also apply to how Council will manage personal, sensitive and health information in relation to its employees.

Certain information is exempt from the provisions of the *Privacy & Data Protection Act* 2014. For instance, publicly available information (as defined in the *Local Government Act* 1989) by its very nature cannot be deemed to be private. Likewise information used for law enforcement is also exempt due to its required use for legal purposes.

The privacy legislation outlined in this policy is in addition to existing statutory and common law obligations that regulate the manner in which Greater Dandenong City Council handles personal Information. In

particular, requirements under the *Freedom of Information Act* 1982 and the *Local Government Act* 1989 will apply.

All requests to access documents held by the Greater Dandenong City Council, need to be made in accordance with the *Freedom of Information Act* 1982**. FOI processes apply to staff for any information which is not readily accessible or routinely shared with them during the normal course of their employment.**

3. References

The primary legislative obligations applying to Council's treatment of personal, sensitive and health information are contained in the Victorian Government's *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*. All relevant legislation, guidelines and sources are listed below:

Victorian Legislation, Principles and other reference sources (as amended or replaced from time to time)

- *Privacy and Data Protection Act* 2014
- *Health Records Act* 2001
- *Health Services Act* 2001
- *Occupational Health & Safety Act* 2004 and related regulations
- *Workplace Injury Rehabilitation and Compensation Act* 2013 and related regulations
- *Freedom of Information Act* 1982
- *Local Government Act* 1989
- *Public Records Act* 1973
- Privacy Victoria Website
- Privacy Victoria publications, guidelines and rulings
- Department of Human Services Website
- Office of the Commissioner for Privacy and Data Protection
- Office of the Health Services Commissioner
- *Criminal Act* 1958

4. Definitions

Personal information — Means information or an opinion about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

Health information — Means information or an opinion about an individual's:

- physical, mental or psychological health (at any time);
- a disability (at any time);
- expressed wishes about the future provision of health services to him or her;
- a health service provided, or to be provided, that is also personal information;
- other personal information collected to provide, or in providing, a health service;

- other personal information collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances;
- other personal information that is genetic information about an individual in a form which is, or could be, predictive of the health (at any time) of the individual or of any of his or her descendants.

Sensitive information Means information or an opinion about an individual's:

- race or ethnic origin;
- political opinions;
- membership of a political association;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record

5. Council Policy

Objectives

Council has implemented practical measures and takes all reasonable steps to ensure full compliance with its obligations under the *Privacy and Data Protection Act* 2014 and the *Health Records Act* 2001 and the Privacy Principles contained in both Acts.

Context/ Rationale

The primary legislative obligations applying to Council's treatment of personal, sensitive and health information are contained in the Victorian Government's *Privacy and Data Protection Act 2014* and the Victorian *Health Records Act 2001*.

The legislation prescribes Information and Health Privacy Principles which are a legally binding set of principles that set the basic standard for which Council must comply with to promote and ensure the fair and responsible collection, storage, usage, disclosure and destruction of personal, sensitive and health information. The following is a list of the Information and Health Privacy Principles:

Principle 1 -Collection
Principle 2 - Use and disclosure
Principle 3 - Data Quality
Principle 4 - Data Security & Data Retention
Principle 5 - Openness
Principle 6 - Access and correction
Principle 7 - Identifiers & Unique identifiers
Principle 8 - Anonymity
Principle 9 - Trans-border data flows

Principle 10 - Sensitive Information

The *Health Records Act* 2001 Principles vary slightly as follows, including an additional Principle:

Principle 10 – Transfer of closure of the practice of a health service provider

Principle 11 – Making information available to another health service provider

See the table in Appendix 1 for details of the full *Health and Information Privacy Principles,* extracted from the *Privacy and Data Protection Act* 2014 and *Health Records Act* 2001.

Health Records Act – www.health.vic.gov.au/hsc
Privacy and Data Protection Act – www.privacy.vic.gov.au

How is Personal and Health Information collected and stored?

Where it is reasonable and practical to do so, Council will collect personal and health information directly from an individual or their authorised representative. This may be in person, in writing, by telephone, or by electronic means such as Council's website.

Council will hold the information it collects on electronic systems, and where necessary, in paper format. Council has an electronic document and records management system that is compliant with current government archival standards and legislation.

All personal and health information stored by Council is protected against unauthorised access, alteration, disclosure or destruction. It is mandatory for all personnel authorised with access to Greater Dandenong City Council systems to ensure the information is kept secure and confidential in accordance with Council policies and procedures.

All personal and health information stored electronically is password protected and all personal and health information stored in paper form is in a locked facility with authorised access only.

Why is Personal and Health Information collected?

Council will only collect personal or health information that is necessary at the time of collection for specific and legitimate functions and activities of Council. Situations in which personal information may be collected include, but are not limited to:

- the processing of registration/membership application forms and any subsequent amendments to those details;
- when dealing with requests or applications for products or services;
- when required by law;

- when dealing with individuals who contact us regarding our activities or services;
- when required to ensure compliance with health and safety obligations; or
- when reasonably necessary to ensure compliance with Council policies and procedures.

When will Personal and Health Information be destroyed?	Personal and health Information stored in paper files that is no longer required is destroyed in accordance with the Public Records Office of Victoria (PROV) - Records Disposal Authority. Personal and health information stored electronically that is no longer required is deleted in a secure manner in accordance with Council policies and procedures. Audit trails are created where personal information is accessed, including amended or deleted records using Council's electronic systems.
How can I access my Personal or Health Information?	Requests to access your personal or health information should be made in writing to Council's Information Privacy Officer. Contact information for Council's Information Privacy Officer is available on Council's website www.greaterdandenong.com. All access to personal and health information is made in accordance with IPP6 and HPP6 *(Access and Correction)*. Written requests for information will be responded to in writing within 10 business days from the date on which it is received by Council. If the information provided by Council is considered by the individual to be inaccurate, out-of-date or incomplete, irrelevant or misleading for the purpose for which it is held, then a request can be made to amend the record in accordance with IPP6 and HPP6 *(Access and Correction)*.
How is Personal and Health Information disclosed?	Personal and health Information held by Council is not disclosed to other agencies or organisations without the consent of the individual or their authorised representative unless required to comply with health and safety obligations or Council policies and procedures or where otherwise required or authorised by law. Where this occurs, it will be disclosed in a manner consistent with the Privacy Principles. Requests for information under the *Freedom of Information Act* 1982 override the provisions of the *Privacy & Data Protection Act* 2014 to the extent of the legislation.
When is Personal and Health Information disclosed to third	Council may have a legal obligation to disclose the personal and/or health information of individuals under the *Privacy and Data Protection Act* 2014, the *Health Records Act* 2001 and other Victorian legislation including, but not limited to, the *Victorian Data Sharing Act* 2017, the *Child Wellbeing*

parties?	*and Safety Act* 2005 and the *Family Violence Protection Act* 2008. Where personal, sensitive and health information has been collected and needs to be passed onto others who are engaged to provide services on behalf of Council, information is only disclosed: • with the consent of the individual or their authorised representative; or • where the individual would reasonably expect, or has been told that, information of that kind is usually passed to those individuals, bodies or agencies. Where personal, sensitive and/or health information has been collected and needs to be passed onto others who are engaged in law enforcement, protective or other services, information is only disclosed: • if the request for disclosure is in writing; • details of the information request are provided; and • the disclosure of the information is authorised by law. Council must maintain a written record of all disclosures made to other agencies. An audit trail (notification) will be created on the specific database advising that personal information has been accessed and shared. This notification will be undertaken in the format specified by the guiding legislation. All third party recipients of personal or health information are required to treat the information in accordance with the Information and Health Privacy Principles outlined in the *Privacy & Data Protection Act* 2014.
Can I remain anonymous?	If a public request is received all individuals will be given the option of not identifying themselves when contacting Council where feasible and lawful. In circumstances where anonymity would impede the ability of the Council to properly provide a service, Council will ensure that individuals are aware of any limitations to services if the information is not provided.
What happens when I access Council's website or use online transactions?	When entering payment information, the transaction occurs directly between an individual's bank and Council's payment gateway providers, Securepay and Australia Post. Council cannot access credit card details. In instances where an individual is required to give personal information in any area of Council's websites, that information is retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Individuals who choose not to provide personal information are still able to access most areas of Council's websites. Council tracks visits to its website and uses the data to analyse for trends and statistics. This process does not collect any personal data or location details in regard to the individual or from where the source information

originated.

Note: Council also has an internal Information Security Policy

What is the role of the Information Privacy Officer?

The Information Privacy Officer (or nominated delegate) handles enquires, complaints or adjustments regarding personal or health information. See below for contact details of the Information Privacy Officer/Health Records Officer.

Written complaints or requests for information will be responded to in writing within 10 business days from the date on which it is received by Council unless the request is covered by the *Freedom of Information Act* 1982.

Is there a complaints/ dispute resolution process?

If Council is alerted to any alleged breach of any of its electronic data base systems which store personal or health information of individuals, it will conduct a thorough and diligent investigation in accordance with its current Information Breach Protocol. This will involve notifying any person that may have been affected by the alleged breach.

If an individual feels aggrieved by Council's handling of personal information, in the first instance, they should lodge any concerns or complaints in writing to Council's Information Privacy Officer.

The Information Privacy Officer
City of Greater Dandenong
PO Box 200
DANDENONG Vic 3175

Tel: 8571 5100

The complainant will be provided with a written response within 10 business days from the date on which it is received by Council.

If the complainant is not satisfied with the response provided by Council they may contact either the Victorian Information Commissioner or the Health Complaints Commission for resolution.

Victorian Information Commissioner
PO Box 24274, Melbourne Victoria 3001
Tel: 1300 006 842
Email: enquiries@ovic.vic.gov.au
Website: www.ovic.vic.gov.au

Health Complaints Commissioner
Level 26, 570 Bourke Street, Melbourne Victoria 3000
Tel: 1300 582 113
Email: hcc@hcc.vic.gov.au
Website: https://hcc.vic.gov.au

6. Related Documents

Related Council documents (as varied from time to time)	• Information Security Policy • Working with Children Check Guidelines • Police Check Policy • Recruitment Policy • Reasonable Adjustment Guidelines • Greater Dandenong City Council Information Breach Protocol • Greater Dandenong City Council Protective Data Security Plans (Committees of Management)

Appendix 1

Information Privacy Principles

IPP 1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(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.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

IPP 2 Use and Disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless –

(a) both of the following apply –

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual –

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information; or

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent –

(i) a serious threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety, or public welfare; or

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(f) the use or disclosure is required or authorised by or under law; or

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(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

(h) the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and –

(i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

Appendix 1

(ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(g), it must make a written note of the use or disclosure

IPP 3 Data Quality

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

IPP 4 Data Security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

IPP 5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

IPP 6 Access and Correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that –

(a) providing access would pose a serious threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders –

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, the organisation –

(a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must –

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information—

as soon as practicable, but no later than 45 days after receiving the request.

IPP 7 Unique Identifiers

7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless –

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless –

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

IPP 8 Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

Appendix 1

IPP 9 Trans-border Data Flows

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if –

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply –

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

IPP 10 Sensitive Information

10.1 An organisation must not collect sensitive information about an individual unless –

(a) the individual has consented; or

(b) the collection is required under law; or

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns –

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if –

(a) the collection –

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

Health Privacy Principles

HPP 1--Collection

<u>When health information may be collected</u>

1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies--

(a) the individual has consented;

(b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law);

(c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent within the meaning of section 85(3) and--

(i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(ii) the individual does not have such an authorised representative;

(d) the information is disclosed to the organisation in accordance with HPP 2.2(a), (f), (i) or (l) or HPP 2.5;

(e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest--

(i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(ii) it is impracticable for the organisation to seek the individual's consent to the collection; and

(iii) the information is collected in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this subparagraph;

(f) the collection is necessary to prevent or lessen--

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare--

and the information is collected in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph;

(g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function;

(h) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(i) the collection is in the prescribed circumstances.

How health information is to be collected

1.2 An organisation must collect health information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 If it is reasonable and practicable to do so, an organisation must collect health information about an individual only from that individual.

1.4 At or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects health information about an individual from the individual, the organisation must take steps that are reasonable in the circumstances to ensure that the individual is generally aware of--

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(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.

1.5 If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is or has been made aware of the matters listed in HPP 1.4 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence.

1.6 An organisation is not required to notify the individual of the identity of persons, or classes of persons, to whom health information may be disclosed in accordance with HPP 2.2(f).

Information given in confidence

1.7 If personal information is given in confidence to a health service provider about an individual by a person other than--

(a) the individual; or

(b) a health service provider in the course of, or otherwise in relation to, the provision of health services to the individual--

with a request that the information not be communicated to the individual to whom it relates, the provider must--

(c) confirm with the person that the information is to remain confidential; and

(d) if the information remains confidential--

(i) record the information only if it is relevant to the provision of health services to, or the care of, the individual; and

(ii) take reasonable steps to ensure that the information is accurate and not misleading; and

(e) take reasonable steps to record that the information is given in confidence and is to remain confidential.

Appendix 1

HPP 2--Use and Disclosure

2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1.

2.2 An organisation must not use or disclose health information about an individual for a purpose (the "**secondary purpose**") other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies:

(a) both of the following apply--

(i) the secondary purpose is directly related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); or

(d) all of the following apply--

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and

(iii) the individual is incapable of giving consent within the meaning of section 85(3) and—

(A) it is not reasonably practicable to obtain the consent of an authorised

representative of the individual within the meaning of section 85; or

(B) the individual does not have such an authorised representative; or

(e) all of the following apply--

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and

(iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and

(iv) the information is used in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(f) the use or disclosure is for the purpose of—

(i) funding, management, planning, monitoring, improvement or evaluation of health services; or

(ii) training provided by a health service provider to employees or persons working with the organisation--

and--

(iii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the individual's consent to the use or disclosure; or

(iv) reasonable steps are taken to de-identify the information--

and--

(v) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(vi) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph; or

(g) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest--

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(iii) the use or disclosure is in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this subparagraph; and

(iv) in the case of disclosure—

(A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and

(B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or

(h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent--

(i) a serious threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety or public welfare—

and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(i) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(j) the organisation reasonably believes that the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(k) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(l) the use or disclosure is in the prescribed circumstances.

Note: Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

2.3 If an organisation discloses health information under paragraph (i) or (j) of HPP 2.2, it must make a written note of the disclosure.

2.4 Despite HPP 2.2, a health service provider may disclose health information about an individual to an immediate family member of the individual if—

(a) either--

(i) the disclosure is necessary to provide appropriate health services to or care of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (a); and

(c) the individual is incapable of giving consent to the disclosure within the meaning of section 85(3); and

(d) the disclosure is not contrary to any wish--

(i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and

(ii) of which the organisation is aware or could be made aware by taking reasonable steps; and

(e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

2.5 Despite HPP 2.2, an organisation may use or disclose health information about an individual where—

(a) it is known or suspected that the individual is dead; or

(b) it is known or suspected that the individual is missing; or

(c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure--

and the use or disclosure is to the extent reasonably necessary--

(d) to identify the individual; or

(e) to ascertain the identity and location of an immediate family member or other relative of the individual for the purpose of--

(i) enabling a member of the police force, a coroner or other prescribed organisation to contact the immediate family member or other relative for compassionate reasons;

or

(ii) to assist in the identification of the individual--

and, in the circumstances referred to in paragraph (b) or (c)--

(f) the use or disclosure is not contrary to any wish--

(i) expressed by the individual before he or she went missing or became incapable of consenting and not withdrawn by the individual; and

(ii) of which the organisation is aware or could have become aware by taking reasonable steps; and

(g) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph.

HPP 3--Data Quality

3.1 An organisation must take steps that are reasonable in the circumstances to make sure that, having regard to the purpose for which the information is to be used, the health information it collects, uses, holds or discloses is accurate, complete, up to date and relevant to its functions or activities.

Appendix 1

HPP 4--Data Security and Retention

4.1 An organisation must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless--

(a) the deletion is permitted, authorised or required by the regulations or any other law; or

(b) the deletion is not contrary to the regulations or any other law and occurs--

(i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or

(ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider--

whichever is the later.

4.3 A health service provider who deletes health information in accordance with HPP 4.2 must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted.

4.4 A health service provider who transfers health information to another individual or organisation and does not continue to hold a record of that information must make a written note of the name and address of the individual or organisation to whom it was transferred.

4.5 An organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by this Act, the regulations made under this Act or any other law.

HPP 5 Openness

5.1 An organisation must set out in a document--

(a) clearly expressed policies on its management of health information; and

(b) the steps that an individual must take in order to obtain access to their health information.

The organisation must make the document available to anyone who asks for it.

5.2 On request by an individual, an organisation must take reasonable steps--

(a) to let the individual know--

(i) whether the organisation holds health information relating to the individual; and

(ii) the steps that the individual should take if the individual wishes to obtain access to the information; and

(b) if the organisation holds health information relating to the individual, to let the individual know in general terms--

(i) the nature of the information; and

(ii) the purposes for which the information is used; and

(iii) how the organisation collects, holds, uses and discloses the information.

HPP 6 Access and Correction

Access

6.1 If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual in accordance with Part 5, unless--

(a) providing access would pose a serious threat to the life or health of any person under section 26 and refusing access is in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(b) providing access would have an unreasonable impact on the privacy of other individuals and refusing access is in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(c) the information relates to existing legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery in those proceedings or is subject to legal professional privilege; or

(d) providing access would reveal the intentions of the organisation in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the organisation unreasonably to disadvantage; or

(e) the information is subject to confidentiality under section 27; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency; or

(j) a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia; or

(k) the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again; or

(l) the individual has been provided with access to the health information in accordance with Part 5 and is making an unreasonable, repeated request for access to the same information in the same way.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the information.

Note: An organisation breaches HPP 6.1 if it relies on HPP 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where HPP 6.2 does not apply.

6.3 If access is refused on the ground that it would pose a serious threat to the life or health of the individual, the procedure in Division 3 of Part 5 applies.

6.4 Without limiting sections 26 and 27, nothing in this Principle compels an organisation to refuse to provide an individual with access to his or her health information.

Correction

6.5 If an organisation holds health information about an individual and the individual is able to establish that the information is inaccurate, incomplete, misleading or not up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date but must not delete the information otherwise than in accordance with HPP 4.2.

6.6 If--

(a) the organisation is not willing to correct the health information in accordance with a request by the individual; and

(b) no decision or recommendation to the effect that the information should be corrected wholly or partly in accordance with the request, is pending or has been made under this Act or any other law; and

(c) the individual gives to the organisation a written statement concerning the requested correction--

the organisation must take reasonable steps to associate the statement with the information.

6.7 If the organisation accepts the need to correct the health information but—

(a) the organisation considers it likely that leaving incorrect information, even if corrected, could cause harm to the individual or result in inappropriate health services or care being provided; or

(b) the form in which the health information is held makes correction impossible; or

(c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so corrected—

the organisation must place the incorrect information on a record which is not generally available to anyone involved in providing health services to the individual, and to which access is restricted, and take reasonable steps to ensure that only the corrected information is generally available to anyone who may provide health services to the individual.

6.8 If an organisation corrects health information about an individual, it must--

(a) if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made; and

(b) take reasonable steps to notify any health service providers to whom the organisation disclosed the health information before its correction and who may reasonably be expected to rely on that information in the future.

6.9 If an individual requests an organisation to correct health information about the individual, the organisation must take reasonable steps to notify the individual of a decision on the request as soon as practicable but in any case not later than 30 days after the request is received by the organisation.

Written reasons

6.10 An organisation must provide written reasons for refusal of access or a refusal to correct health information.

Appendix 1

HPP 7 Identifiers

7.1 An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

7.2 Subject to HPP 7.4, a private sector organisation may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if--

(a) the individual has consented to the adoption of the same identifier; or

(b) the use or disclosure of the identifier is required or authorised by or under law.

7.3 Subject to HPP 7.4, a private sector organisation may only use or disclose an identifier assigned to an individual by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if--

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more of paragraphs (c) to (l) of HPP 2.2; or

(b) the individual has consented to the use or disclosure; or

(c) the disclosure is to the public sector organisation which assigned the identifier to enable the public sector organisation to identify the individual for its own purposes.

7.4 If the use or disclosure of an identifier assigned to an individual by a public sector organisation is necessary for a private sector organisation to fulfil its obligations to, or requirements of, the public sector organisation, a private sector organisation may either--

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector organisation; or

(b) use or disclose an identifier of the individual that has been assigned by the public sector organisation.

HPP 8 Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

HPP 9 Transborder Data Flows

9.1 An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if--

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply--

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles; or

(g) the transfer is authorised or required by any other law.

HPP 10 Transfer or closure of the practice of a health service provider

10.1 This Principle applies if the practice or business of a health service provider (**"the provider"**) is to be--

(a) sold or otherwise transferred and the provider will not be providing health services in the new practice or business; or

(b) closed down.

10.2 The provider or, if the provider is deceased, the legal representatives of the provider, must--

(a) publish a notice in a newspaper circulating in the locality of the practice or business stating--

(i) that the practice or business has been, or is about to be, sold, transferred or closed down, as the case may be; and

(ii) the manner in which the provider proposes to deal with the health information held by the practice or business about individuals who have received health services from the provider, including whether the provider proposes to retain the information or make it available for transfer to those individuals or their health service providers;

and

(b) take any other steps to notify individuals who have received a health service from the provider in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph.

10.3 Not earlier than 21 days after giving notice in accordance with HPP 10.2, the person giving the notice must, in relation to health information about an individual held by, or on behalf of, the practice or business, elect to retain that information or transfer it to--

(a) the health service provider, if any, who takes over the practice or business; or

(b) the individual or a health service provider nominated by him or her.

10.4 A person who elects to retain health information must continue to hold it or transfer it to a competent organisation for safe storage in Victoria, until the time, if any, when the health information is destroyed in accordance with HPP 4.

10.5 Subject to HPP 10.2, a person must comply with the requirements of this Principle as soon as practicable.

10.6 Despite any other provision of the Health Privacy Principles, a person who transfers health information in accordance with this Principle does not, by so doing, contravene the Health Privacy Principles.

10.7 If—

(a) an individual, in response to a notice published under HPP 10.2, requests that health information be transferred to him or her or to a health service provider nominated by him or her; and

(b) the person who published the notice elects to retain the health information

the request must be taken to be--

(c) in the case of a request that the health information be transferred to him or her, a request for access to that health information in accordance with Part 5 or HPP 6; and

(d) in the case of a request that the health information be transferred to a health service provider nominated by him or her, a request for the transfer of that health information in accordance with HPP 11--

and it must be dealt with in accordance with this Act.

10.8 This Principle operates subject to any other law, including the **Public Records Act 1973**.

10.9 For the purposes of HPP 10.1(a), a business or practice of a provider is transferred if--

(a) it is amalgamated with another organisation; and

(b) the successor organisation which is the result of the amalgamation is a private sector organisation.

HPP 11 Making information available to another health service provider

11.1 If an individual--

(a) requests a health service provider to make health information relating to the individual held by the provider available to another health service provider; or

(b) authorises another health service provider to request a health service provider to make health information relating to the individual held by that provider available to the requesting health service provider--

a health service provider to whom the request is made and who holds health information about the individual must, on payment of a fee not exceeding the prescribed maximum fee and subject to the regulations, provide a copy or written summary of that health information to that other health service provider.

11.2 A health service provider must comply with the requirements of this Principle as soon as practicable.

11.3 Nothing in Part 5 or HPP 6 limits the operation of this Principle.

11.4 For the purposes of HPP 10.7, this Principle applies to a legal representative of a deceased health service provider in the same way that it applies to a health service provider.