SCHEDULES

SCHEDULE 1

THE INFORMATION PRIVACY PRINCIPLES

In these Principles—

sensitive information means information or an opinion about an individual's—

(a) racial or ethnic origin; or

(b) political opinions; or

(c) membership of a political association; or

(d) religious beliefs or affiliations; or

(e) philosophical beliefs; or

(f) membership of a professional or trade association; or

(g) membership of a trade union; or

(h) sexual preferences or practices; or

(i) criminal record—

that is also personal information;

unique identifier means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name but does not include an identifier within the meaning of the **Health Records Act 2001**.

1 Principle 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 the individual 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.

2 Principle 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 and imminent 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 Organisation (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

(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 IPP 2.1(g), it must make a written note of the use or disclosure.

3 Principle 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.

4 Principle 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.

5 Principle 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.

6 Principle 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 and imminent 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 IPP 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.

7 Principle 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 IPP 2.1(d) to (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.

8 Principle 8—Anonymity

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

9 Principle 9—Transborder 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 precontractual 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.

10 Principle 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 and imminent 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.

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 the personal information is collected in the context of the delivery of an emergency service.

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

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

(ea) all of the following apply—

(i) ASIO has asked the agency to disclose the personal information;

(ii) an officer or employee of ASIO authorised in writing by the director-general of ASIO for this paragraph has certified in writing that the personal information is required in connection with the performance by ASIO of its functions;

(iii) the disclosure is made to an officer or employee of ASIO authorised in writing by the director-general of ASIO to receive the personal information; 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 by 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.