



The Mailing House Pty Limited
ABN 45 003 061 729
Unit A, 10-16 South Street
RYDALMERE NSW 2116
Ph: (61 2) 8845 6000
Fax: (61 2) 9684 4322
P.O. Box 255
RYDALMERE NSW 1701
Email: tmh@mailinghouse.com.au
WHOLLY AUSTRALIAN OWNED

PRIVACY POLICY - THE MAILING HOUSE PTY LIMITED

This document is to be read in conjunction with the National Privacy Principles (see annexure E) and the Sept 2001 Guidelines to the National Privacy Principles and Information Sheets published by the Office of the Federal Privacy Commissioner.

Abbreviated References:

National Privacy Principles (NPP's)

Office of the Federal Privacy Commissioner (OFPC)

The Mailing House Pty Limited (TMH)

The Privacy Amendment (Private Sector) Act 2000 (The Act)

Index:

Page	Subject
2	Privacy Policy
4	Annexure A- Letter of Guarantee
5	Annexure B - Policy Document – Security of list data
6	Annexure C - Procedure – Building Security
7	Annexure D - Summary of NPP Obligations
9	Annexure E – National Privacy Principles
18	Annexure F – Key Concepts & Glossary

For any further information regarding this policy document contact The Privacy Officer at any of the above contact addresses or numbers.

This document does not express a legal opinion and any person or organisation is urged to seek advice from their legal advisors with regard to the implementation of The Privacy Amendment (Private Sector) Act 2000

Preamble: The Mailing House (TMH) is bound by The Act.

The Mailing House may collect personal information as part of the collection of client details for the primary purpose of administration and communication of jobs we undertake on behalf of our customers. Any personal data such as name, address, telephone numbers, fax and email would only be volunteered by the individual to assist communication as a means to expedite their projects.

The Mailing House's primary business is to receive from clients, databases containing personal information, which from time to time may comprise sensitive information. Under our client's instructions we prepare personalised direct mail communications for distribution, mainly by post, to each persons address.

The Mailing House and its subsidiary company MailCom Data Entry Services, as a contractor, does collect and store personal information on behalf of and on the instruction of clients. See Information Sheet 8 – 2001 for specific obligations.

This Privacy Policy document details the steps taken to comply with the National Privacy Principles (NPP's). Most NPP's are the responsibility of our clients. We endeavour to advise our clients about their responsibility under The Act.

NPP 1 Collection: NPP 10 Sensitive Information:

TMH only collects personal information as instructed by our clients. This information is supplied by the client, and only used under the client's specific instructions and stored on their behalf, or destroyed, or returned to the them.

NPP 2 Use & Disclosure:

TMH would not use or disclose any information other than at the express instructions of our clients. Our standard **Letter of Guarantee (Annexure A)** states the TMH policy concerning Use & Disclosure of client's information.

NPP 3 Data Quality:

Our high levels of professional service require us to record information as accurately as possible. This accuracy will only be limited by the standard of the data presented for capture and the accuracy of the data entry operators. TMH has developed many software routines to ensure that all data is correctly processed and not altered or corrupted during any process.

It is the ultimate responsibility of the owner of the information (our client) to ensure the data is complete, accurate and up to date.

NPP 4 Data Security:

TMH takes all reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, inappropriate modification and disclosure.

These steps include a secure area where any personal information data files may be held. The site is protected by a 'back to base' security system.
See **Procedure Building Security** (*Annexure C*).

Computer and Network security is achieved by use of passwords for each staff member, external firewalls and virus protection.

Every staff member who may have any role in the processing of personal information has been instructed in the company's Security Policy and has signed the company's **Security of List Data Agreement** (*Annexure B*), which is held as part of their personnel record.

NPP 5 Openness:

This policy Document complies with NPP5. TMH is bound by the NPP's. TMH seeks exemption for any personal information that is held as part of personnel records.

Any individual seeking information about The Privacy Policy of TMH can contact The Privacy Officer at TMH at any of the contact points listed on the first page.

NPP 6 Access & Correction:

Any access or correction to personal information held on behalf of our clients would need to be directed through that client. TMH would then comply in the spirit of NPP6 as directed by our client.

NPP 7 Identifiers:

Appropriate staff have been briefed to ensure that any Commonwealth government identifier (EG Tax File Number, Social Security number) or for that matter state government identifier (eg driver's licence) is not used as an identifier or displayed where it could be disclosed to other than the intended recipient.

This also applies to other non government identifiers such as Securityholder Reference Number as related to an individual's share ownership.

NPP 8 Anonymity:

Where practicable we would deal with people anonymously.

NPP 9 Transborder Data Flows:

TMH would brief our clients as to their obligations under NPP9 should they instruct TMH to transfer personal information outside Australia.

LETTER OF GUARANTEE

TO:

RE: PROCESSING OF MAILING FILES RECEIVED FROM YOUR ORGANISATION

The following terms are fully understood and will be upheld by us on your behalf.

1. We agree to accept from you, computer files and agree they will not be used by us other than for the specific mailing purpose described in the mailing brief.
2. No copy, duplicate or extracts of the list will be made other than is necessary for the purpose of performing the clients' requirements. No such copies shall be retained but shall be immediately deleted on completion of such processing.
3. No 'enhancement' of any other list or database by the use of the list/s referred to herein shall be undertaken by us without written agreement expressly permitting such 'enhancement'.
4. We understand that the said list/s have been seeded with 'dummy' names and addresses and the receipt of any one envelope and/or offer from us, our subsidiaries or clients, other than the sample of the agreed specific mail piece addresses to any such 'dummy' names within the list/s, shall be accepted as proof of misuse of the list/s.
5. We agree to deliver to your organisation at our expense, names and addresses (in their original form) returned to our address as undeliverables (DLO's).
6. We agree to return to you all files upon written termination by either party of our association.

Signed for and on behalf of
THE MAILING HOUSE
UNIT A, 10 - 16 SOUTH STREET
RYDALMERE NSW 2116

SIGNATURE:
NAME:
TITLE:
DATE:

Signed for and on behalf of

SIGNATURE:
NAME:
TITLE:
DATE:

The Mailing House is bound by The Privacy Amendment (Private Sector) Act 2000 and has a Privacy Policy available upon request.

The Mailing House has in place Security Agreements with most of the companies who supply data to us. These comprise **List Brokers** and **List Owners** such as Drake, Dun & Bradstreet, Marketing Orientations and our many **individual clients**.

Lists supplied by **individual clients** are for the exclusive use of that client. You are not allowed to merge it with other data unless authorised by the client to do so. In the case of a client's list you are authorised to produce whatever the client requests by way of listings, magnetic media etc.

In the case of rental lists supplied by a **List Broker** for the one time use by a client, we are not allowed to produce additional copies of the data. We are only allowed to produce one (1) set of labels or laser letters or ink jet diskette etc. We are not allowed to produce a line listing to be given to the client for them to check or use as a response recording device. Nor are we permitted to email rental list data to the client. This can only be done by written consent of the **List Owner** or **List Broker**.

We have Security Agreements with various **List Brokers** and **List Owners** where we have agreed to abide with their regulations and the most important item in those agreements concerns the creation of copies of the data.

In processing jobs we make internal copies of the data. Conversions, de-duplications, upper to lower case routines, all create a new file, however at the end of the job, these files must not be kept for inclusion into any other job.

If a client wishes to use a list a number of times then they have to pay an additional rental fee. Typically, twice the rental fee entitles them to own the list and they can use it as often as they like. This fee varies with **List Owners**.

Due to the above requirements **List Owners** will not release lists to clients. Rental lists are only released to mailing houses who agree to be bound by these rules.

To detect unauthorised use of a mailing list most **List Owners** have inserted 'seed' names into the list. These names have been constructed in such a way that they could not genuinely be created, hence mail addressed to that person is deemed to be proof of the use of the list. If unauthorised mail is received then they have a case to follow up.

**THE MAILING HOUSE POLICY IS:
'NO COPIES WITHOUT WRITTEN CONSENT OF THE LIST OWNER'**

Name: Signed: Date:

The Mailing House is bound by The Privacy Amendment (Private Sector) Act 2000 and has a Privacy Policy available upon request.

Annexure D

Summary of NPP obligations from the Sept 2001 Guidelines*

- ❑ If it is lawful and practicable to do so, give people the option of interacting anonymously with you.
- ❑ Only collect personal information that is necessary for your functions or activities.
- ❑ Use fair and lawful ways to collect personal information.
- ❑ Collect personal information directly from an individual if it is reasonable and practicable to do so.
- ❑ Get consent to collect sensitive information unless specified exemptions apply.
- ❑ At the time you collect personal information or as soon as practicable afterwards, take reasonable steps to make an individual aware of:
 - why you are collecting information about them;
 - who else you might give it to; and
 - other specified matters.
- ❑ Take reasonable steps to ensure the individual is aware of this information even if you have collected it from someone else.
- ❑ Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in NPP 2.1 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances). Note that;
 - If the information is sensitive the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related and the direct marketing provisions of NPP 2.1(c) do not apply.
- ❑ Take reasonable steps to ensure the personal information you collect, use or disclose is accurate, complete and up-to-date. This may require you to correct the information.
- ❑ Take reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure.
- ❑ Take reasonable steps to destroy or permanently de-identify personal information if you no longer need it for any purpose for which you may use or disclose the information.
- ❑ Have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it.
- ❑ If an individual asks, take reasonable steps to let them know, generally, what sort of personal information you hold, what purposes you hold it for and how you collect, use and disclose that information.

- If an individual asks, you must give access to the personal information you hold about them unless particular circumstances apply that allow you to limit the extent to which you give access – these include emergency situations, specified business imperatives and law enforcement or other public interests.
- Only adopt, use or disclose a Commonwealth Government identifier if particular circumstances apply that would allow you to do so.
- Only transfer personal information overseas if you have checked that you meet the requirements of NPP 9.

*This is a summary only and NOT a full statement of obligations. These are set out in the NPP's themselves.

National Privacy Principles

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) the organisations (or the types of 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 subclause 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 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 information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

- (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
 - (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
 - (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
- (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) 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 or safety; or
 - (ii) a serious threat to public health or public safety; or
- (f) 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
- (g) the use or disclosure is required or authorised by or under law; or
- (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (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 or prescribed conduct;

- (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.
- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
 - (a) the individual:
 - (i) is physically or legally incapable of giving consent to the disclosure; or
 - (ii) physically cannot communicate consent to the disclosure; and
 - (b) a natural person (the *carer*) providing the health service for the organisation is satisfied that either:
 - (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - (ii) the disclosure is made for compassionate reasons; and
 - (c) the disclosure is not contrary to any wish:
 - (i) expressed by the individual before the individual became unable to give or communicate consent; and
 - (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
 - (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).
- 2.5 For the purposes of subclause 2.4, a person is *responsible* for an individual if the person is:
 - (a) a parent of the individual; or
 - (b) a child or sibling of the individual and at least 18 years old; or
 - (c) a spouse or de facto spouse of the individual; or
 - (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
 - (e) a guardian of the individual; or
 - (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

- (g) a person who has an intimate personal relationship with the individual; or
- (h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

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 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 for which the information may be used or disclosed under National Privacy Principle 2.

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 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) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

- (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
- (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- (d) the request for access is frivolous or vexatious; or
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- (f) 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
- (g) providing access would be unlawful; or
- (h) denying access is required or authorised by or under law; or
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed 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 an enforcement body; or
- (k) an enforcement body 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.

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

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 (k) (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, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

- 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.

7 Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
- (a) an agency; or
 - (b) an agent of an agency acting in its capacity as agent; or
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

- 7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

- 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
 - (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

- 7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an **identifier**.

8 Anonymity

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

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country 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 National 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 such 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 National Privacy Principles.

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 by 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) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

- (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
- (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

- (a) the information is necessary to provide a health service to the individual; and
- (b) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

- (a) the collection is necessary for any of the following purposes:
 - (i) research relevant to public health or public safety;
 - (ii) the compilation or analysis of statistics relevant to public health or public safety;
 - (iii) the management, funding or monitoring of a health service; and
- (b) 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
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

Key concepts & Glossary

This only includes some of the concepts and terms in the NPP's. If you cannot find a term here you should find it in section 6 of the Privacy Act which is linked at www.privacy.gov.au on the Office's web site. Where terms are defined in the Privacy Act, the relevant section is indicated.

Access

This involves an organisation giving an individual information about themselves held by the organisation. Giving access may include allowing an individual to inspect personal information or giving a copy of it to them.

Children and young people

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. Determining the decision-making capabilities of a young person can be a complex matter, often raising other ethical and legal issues. Organisations will need to address each case individually.

As a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity or understanding to do so themselves. It should be noted that in some states, contracts with people under the age of 18 are not valid.

It may be desirable for organisations that target children or young people to specifically address issues of consent and rights of access to the personal information of children and young people in the information policy that NPP 5 requires them to have. Such a policy might contain general guidelines about how the organisation will make decisions relating to young people and children and the factors it will take into account. The policy might also deal with parental involvement, particularly factors that would indicate that a parent should be involved in the decision-making process.

Collection

An organisation collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when an organisation keeps personal information it has come across by accident or has not asked for.

Consent

Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.

Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise. Competence means that individuals are capable of understanding issues, forming views based on reasoned judgments and communicating their decisions. The general law about competence and incapacity will apply to the issue of consent.

Contractors

The Privacy Act treats the acts and practices of employees (and those 'in the service of' an organisation) in performing their duties of employment as those of the organisation (see section 8(1)(a)). Contractors performing services for an organisation are not considered to fall within this provision. However, where there is a particularly close relationship between an organisation and a contractor it may mean that the actions of the contractor could be treated as having been done by the organisation for the purposes of section 8 of the Privacy Act.

When the parties to a contract are regarded as separate entities under the Privacy Act an organisation that gives personal information to a contractor it is disclosing information and the contractor is collecting the information. In practical terms, this means that the organisation may need to have clauses in the contract for the protection of personal information the organisation discloses to the contractor in order to meet its obligations under the NPP's.

Where the contractor is not an 'organisation' for the purposes of the Privacy Act and so not covered by the NPP's it would be advisable for the organisation to take measures to protect the personal information it discloses to the contractor.

What are reasonable steps under NPP 1.3 and NPP 1.5 for the organisation and a contractor may depend on the nature of the relationship between the organisation and the contractor, including the contractual provisions in place.

For more information about how the NPP's apply where an organisation contracts out a function or activity to a separate entity see *Information Sheet 8 - 2001 Contractors*.

Direct marketing

This allows organisations to use non-sensitive personal information for direct marketing where, among other things, it is impracticable to seek the individual's consent and where the individual is told that they can opt out of receiving any more marketing from the organisation.

This principle only applies to the use of non-sensitive information for direct marketing and does not permit an organisation to disclose personal information for the purpose of direct marketing.

(Impracticable to seek consent)

Considering whether it is impracticable to seek the individual's consent involves balancing a number of factors that could include:

- how often the organisation is in contact with an individual;
- the way an organisation communicates with an individual;
- the consequences for the individual of receiving the information without having consented; and
- the cost to the organisation of seeking consent.

The question of impracticability would generally be considered at the time of the proposed use of the personal information for direct marketing – not the time the personal information was collected.

As the cost of emailing is negligible, ordinarily it will not be 'impracticable' to seek consent where an organisation chooses on-line methods of contact or communication. This means that generally an organisation could not rely on NPP 2.1(c) for techniques such as email marketing or SMS marketing. The option of using 2.1(b) is still available. However, in most cases, this will require express consent.

Disclosure

In general terms an organisation discloses personal information when it releases information to others outside the organisation. It does not include giving individuals information about themselves (this is 'access' see above).

Enforcement body

Enforcement bodies are listed in the definitions in section 6(1) of the Privacy Act. They are also listed in *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement*.

Organisation

The NPP's apply to businesses and bodies that fall within the definition of 'organisation' in section 6C of the Privacy Act. Section 6C says that 'organisation' means: an individual; or a body corporate; or a partnership; or any other unincorporated association; or a trust; that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.'

Personal information

Personal information is information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion (section 6). It includes all personal information regardless of its source.

Personal information relates to a natural living person. A natural person is a human being rather than, for example, a company, which may in some circumstances be recognised as a legal 'person' under the law.

The NPP's apply to the collection of personal information by an organisation for inclusion in a record or a generally available publication, but apart from this, the NPP's only apply to personal information an organisation has collected that it holds in a record.

Primary purpose

Determining the primary purpose of collection should always be possible. Where an organisation collects personal information directly from the individual the context in which the individual gives the information to the organisation will help identify the primary purpose of collection. When an individual provides and an organisation collects personal information, they almost always do so for a particular purpose – for example, to buy or sell a particular product or receive a service. This is the primary purpose of collection even if the organisation has some additional purposes in mind.

How broadly an organisation can describe the primary purpose will need to be determined on a case-by-case basis and it will depend on the circumstances.

Where an organisation collects personal information indirectly a guide to its primary purpose of collection could be what the organisation does with the information soon after it first receives it.

(Related and directly related purposes within reasonable expectations)

To be related, the secondary purpose must be something that arises in the context of the primary purpose.

If personal information is sensitive information the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose for collection.

(Individual's reasonable expectations)

The test for what the individual would 'reasonably expect' would be applied from the point of view of what an individual with no special knowledge of the industry or activity involved would expect.

The NPP's are not intended to prevent personal information about individuals acting in a business capacity from being exchanged in the normal course of a business. In these circumstances, ordinarily it is likely to be within individuals' reasonable expectations that information about them in their business role will be used and disclosed for generally accepted business purposes. For example, exchange of business cards and use of them for later business contacts would ordinarily be consistent with the NPP's.

Related body corporate

A related body corporate is defined in section 50 of the *Corporations Act 2001* (Cth) to mean that where a body corporate is:

- a holding company of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate;

the first mentioned body and the other body are related to each other.

Secondary use and disclosure with consent

This allows an organisation to use or disclose personal information for a secondary purpose if it has the individual's consent. Consent to the use or disclosure can be express or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. For example, it may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up. If the organisation's use or disclosure has serious consequences for the individual, the organisation would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the organisation to seek express consent.

Sensitive information

Sensitive information is a subset of personal information. It means information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information about an individual (section 6).

Use

In general terms, use of personal information refers to the handling of personal information within an organisation including 'the inclusion of information in a publication'.