

# AUSTRALIAN COLLEGE OF PHARMACY PRACTICE & MANAGEMENT

## PRIVACY POLICY

### **1. Authority**

- 1.1 The Council of the Australian College of Pharmacy Practice & Management approved this Privacy Policy on 25 January 2002.
- 1.2 This policy relates to the operations of the College. It supplements information contained in the Privacy Act and is based on the National Privacy Principles for the Fair Handling of Personal Information (NPPs).

### **2. Privacy Policy – simplified statement for members and staff of ACPPM**

- 2.1 We will only collect information that is necessary for what we do.
- 2.2 We will be fair in the way we collect information about you.
- 2.3 We will tell you who we are and what we intend to do with information about you.
- 2.4 Where practicable, we will collect personal information directly from you.
- 2.5 If we collect information about you from someone else we will, wherever possible, make sure you know we have done this.
- 2.6 We will only use or disclose information about you in ways that are consistent with your expectations or are required in the public interest.
- 2.7 We will ensure that information about you is accurate when we collect or use it.
- 2.8 We will keep information about you secure.
- 2.9 We will be open with you about what kinds of personal information we hold and what we do with it.
- 2.10 Wherever possible we will let you see the information we hold about you and correct it if it is wrong.
- 2.11 We will limit our use of identifiers that government agencies have assigned to you.
- 2.12 If we can (and you want us to) we will deal with you anonymously.
- 2.13 We will take steps to protect your privacy if we send personal information about you to a third party.
- 2.14 We will limit the collection of highly sensitive information about you.

### **3. Definitions**

- 3.1 *ACPPM* is the Australian College of Pharmacy Practice & Management.
- 3.2 *CEO* is the Registrar and Chief Executive Officer (CEO) of the ACPPM.
- 3.3 *Collection* is the act of gathering, acquiring, or obtaining personal information from any source, including third parties, by any means and does not include the receipt of unsolicited information.

- 3.4 **Consent** is free and informed agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organisation seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.
- 3.5 **Correct** means, in relation to personal information, to alter that information by way of amendment, deletion or addition.
- 3.6 **Disclosure** is the making available of personal information to others outside the organisation, other than the subject or the information. Disclosure includes publication of personal information through any medium.
- 3.7 **Enforcement agency** means a police force or service of a State or Territory, an agency, to the extent that it is responsible for administering, or performing a function under a law imposing a penalty or sanction, or an agency, to the extent that it is responsible for the administration of a law relating to the protection of the public revenue.
- 3.8 **Generally available publication** means a publication (whether in paper or electronic form) that is generally available to members of the public.
- 3.9 **Health information** is a subset of *sensitive information* and relates to any details of the health or medical condition of the individual.
- 3.10 **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 the individual's name.
- 3.11 **Individual** means a natural person.
- 3.12 **Organisation** means an association, business, charitable organisation, club, government body, institution, professional practice, union, corporation, group of bodies corporate that are related within the meaning of the Corporations Law, or any other collective entity. 'Organisation' includes a sole trader or other individual (for example, a professional or freelance consultant) in his or her business capacity.
- 3.13 **Personal Information** is information (whether fact, opinion or evaluative material), that is recorded in any form 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, but does not include information contained in a generally available publication.
- 3.14 **Reasonable steps** are such steps (if any) as are, in the circumstances, reasonable.
- 3.15 **Registrar** is the Chief Executive Officer (CEO) is the CEO of ACPPM.
- 3.16 **Sensitive Information** is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, membership of a professional or trade association or a trade union, sexual preferences or practices, criminal record or health information about an individual. To be categorised as *sensitive information* the information must also be *personal information*.
- 3.17 **Seriously improper conduct** means corruption, a serious abuse of power, a serious dereliction of duty, or any other seriously reprehensible behaviour.
- 3.18 **Subject of the information**, in relation to personal information, means the individual to whom the information relates.
- 3.19 **Third party**, in relation to personal information, means a person or body other than the ACPPM and the individual who is the subject of the information.
- 3.20 **Use** refers to the treatment and handling of personal information within an organisation.

#### **4. Collection (NPP 1)**

- 4.1 Personal information will not be collected unless the information is necessary for one or more of ACPPM's functions or activities.
- 4.2 Personal information will only be collected by lawful and fair means and not in an unreasonably intrusive way.
- 4.3 At or before the time (or, if that is not practicable, as soon as practicable after) personal information about an individual is collected from the individual, reasonable steps will be taken to ensure that the individual is aware of:
  - 4.3.1 the identity of the ACPPM and how to contact it; and
  - 4.3.2 the fact that the individual is able to gain access to the information; and
  - 4.3.3 the purposes for which the information is collected; and
  - 4.3.4 the organisations (or the types of organisations) to which information is usually disclosed; and
  - 4.3.5 any law that requires the particular information to be collected; and
  - 4.3.6 the main consequences (if any) for the individual if all or part of the information is not provided.
- 4.4 The form of advice to members of the ACPPM is detailed at paragraph 14.1.
- 4.5 Whenever it is reasonable and practicable to do so, personal information about an individual will be collected only from that individual.
- 4.6 If personal information about an individual is collected from someone else, reasonable steps will be taken to ensure that the individual is or has been made aware of the matters listed in paragraph 4.3 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.

#### **5. Use and Disclosure (NPP 2)**

- 5.1 Personal information about an individual will not be used or disclosed for a purpose (the *secondary purpose*) other than the primary purpose of collection unless:
  - 5.1.1 both of the following apply:
    - 5.1.1.1 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;
    - 5.1.1.2 the individual would reasonably expect the use or disclosure for the secondary purpose; or
  - 5.1.2 the individual has consented to the use or disclosure; or
  - 5.1.3 if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
    - 5.1.3.1 it is impracticable to seek the individual's consent before that particular use; and
    - 5.1.3.2 no charge will be levied to the individual for giving effect to a request by the individual not to receive direct marketing communications; and
    - 5.1.3.3 the individual has not made a request not to receive direct marketing communications; and
    - 5.1.3.4 the individual has the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications; or

- 5.1.4 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:
  - 5.1.4.1 it is impracticable to seek the individual's consent before the use or disclosure; and
  - 5.1.4.2 the use or disclosure is conducted in accordance with guidelines approved by the Privacy Commissioner; and
  - 5.1.4.3 in the case of disclosure, the ACPPM reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- 5.1.5 the ACPPM reasonably believes that the use or disclosure is necessary to lessen or prevent:
  - 5.1.5.1 a serious and imminent threat to an individual's life, health or safety; or
  - 5.1.5.2 a serious threat to public health or public safety; or
- 5.1.6 the ACPPM 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
- 5.1.7 the use or disclosure is required or authorised by or under law; or
- 5.1.8 the ACPPM 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:
  - 5.1.8.1 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;
  - 5.1.8.2 the enforcement of laws relating to the confiscation of the proceeds of crime;
  - 5.1.8.3 the protection of the public revenue;
  - 5.1.8.4 the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
  - 5.1.8.5 the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.
- 5.1.9 The ACPPM will lawfully co-operate with agencies performing law enforcement functions in the performance of their functions. This policy does not override any existing legal obligation not to disclose personal information. Nothing in this policy requires the disclosure of personal information and the ACPPM is entitled not to disclose personal information in the absence of a legal obligation to do so.
  - 5.1.9.1 If personal information is used or disclosed under paragraph 5.1.8, a written note of the use or disclosure will be made.
  - 5.1.9.2 Personal information collected from a related organisation will be dealt with as though the information was collected from the individual.

## **6. Data Quality (NPP 3)**

- 6.1 Reasonable steps will be made to ensure that the personal information collected, used or disclosed is accurate, complete and up-to-date.

## **7. Data Security (NPP 4)**

- 7.1 Reasonable steps will be taken to protect any personal information from misuse and loss and from unauthorised access, modification or disclosure.
- 7.2 Reasonable steps will be taken 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 section 5 above (NPP 2).

## **8. Openness (NPP 5)**

- 8.1 This policy document sets out the Society's policies on its management of personal information. This policy document is available to anyone who asks for it.
- 8.2 On request by a member or an employee, the ACPPM will take reasonable steps to advise, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.
- 8.3 The "*simplified statement*" of Privacy Policy (Section 2 of this policy) will be published at least annually in the ACPPM's journal, the *Pharmacy Rising*. The statement at paragraph 14.1 of this policy will be included in membership application and renewal forms. The full Privacy Policy will be published on the ACPPM's web page.

## **9.0 Access and Correction (NPP 6)**

- 9.1 Any personal information held about an individual will be provided to that individual on request by the individual, except to the extent that:
  - 9.1.1 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
  - 9.1.2 in the case of health information-providing access would pose a serious threat to the life or health of any individual; or
  - 9.1.3 providing access would have an unreasonable impact upon the privacy of other individuals; or
  - 9.1.4 the request for access is frivolous or vexatious; or
  - 9.1.5 the information relates to existing or anticipated legal proceedings between the ACPPM and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
  - 9.1.6 providing access would reveal the intentions of the ACPPM in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
  - 9.1.7 providing access would be unlawful; or
  - 9.1.8 denying access is required or authorised by or under law; or
  - 9.1.9 providing access would be likely to prejudice an investigation of possible unlawful activity; or
  - 9.1.10 providing access would be likely to prejudice:
    - 9.1.10.1 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
    - 9.1.10.2 the enforcement of laws relating to the confiscation of the proceeds of crime; or
    - 9.1.10.3 the protection of the public revenue; or
    - 9.1.10.4 the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
    - 9.1.10.5 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

- 9.1.11 an enforcement body performing a lawful security function asks the ACPPM not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.
- 9.2 However, where providing access would reveal evaluative information generated within the ACPPM in connection with a commercially sensitive decision-making process, the individual may be given an explanation for the commercially sensitive decision rather than direct access to the information. This provision will not be relied on to deny access where a commercially sensitive process does not apply.
- 9.3 If access to the information is not required because of one or more of paragraphs 9.1.1 to 9.1.11 (inclusive), if reasonable, the use of mutually agreed intermediaries would be considered to allow sufficient access to meet the needs of both parties.
- 9.4 A charge will not be levied to provide access to personal information.
- 9.5 If an individual is able to establish that any information held is not accurate, complete and up-to-date, reasonable steps will be taken to correct the information so that it is accurate, complete and up-to-date.
- 9.6 If the individual and the ACPPM disagree about whether any information is accurate, complete and up-to-date, and the individual asks the ACPPM to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, reasonable steps will be taken to do so.
- 9.7 Reasons for denial of access or a refusal to correct personal information will be provided.

## **10. Identifiers (NPP 7)**

- 10.1 A membership number will be allocated to each member as an identifier of that member for the purposes of the ACPPM's operations.
- 10.2 An identifier assigned to an individual by another agency or body will not be used or disclosed, unless required by paragraph 5.1.
- 10.3 An individual's name is not an identifier.

## **11. Anonymity (NPP 8)**

- 11.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with the ACPPM.

## **12. Transborder Data Flows (NPP 9)**

- 12.1 Personal information about an individual may be transferred to someone (other than the ACPPM or the individual) who is in a foreign country only if:
  - 12.1.1 the ACPPM 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
  - 12.1.2 the individual consents to the transfer; or
  - 12.1.3 the transfer is necessary for the performance of a contract between the individual and the ACPPM, or for the implementation of pre-contractual measures taken in response to the individual's request; or
  - 12.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the ACPPM and a third party; or
  - 12.1.5 all of the following apply:

- 12.1.5.1 the transfer is for the benefit of the individual;
- 12.1.5.2 it is impracticable to obtain the consent of the individual to that transfer;
- 12.1.5.3 if it were practicable to obtain such consent, the individual would be likely to give it; or
- 12.1.5.4 reasonable steps have been taken to ensure that the information which has been transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

### **13. Sensitive Information (NPP 10)**

- 13.1 Sensitive information about an individual will not be collected unless:
  - 13.1.1 the individual has consented; or
  - 13.1.2 the collection is required by law; or
  - 13.1.3 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:
    - 13.1.3.1 is physically or legally incapable of giving consent to the collection; or
    - 13.1.3.2 physically cannot communicate consent to the collection; or
  - 13.1.4 if the information is collected in the course of the activities of the ACPPM and relates solely to the members of the ACPPM or to individuals who have regular contact with it in connection with its activities and at or before the time of collecting the information, the ACPPM undertakes to the individual whom the information concerns that the ACPPM will not disclose the information without the individual's consent; or
  - 13.1.5 the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 13.2 Health information about an individual will normally only be collected in the course of employment.

### **14. Statement to Members – Collection of Information**

- 14.1 On membership application and renewal forms, the following statement will be included:

*The Australian College of Pharmacy Practice & Management (ACPPM) maintains a database of names, addresses and other information relevant to membership of ACPPM. This data is accessed by ACPPM staff to mail information including publications and member services. It is made available to related organisations, for example the Pharmacy Society of Australia and to companies and organisations which provide member services and benefits. This includes mailing houses that provide these services. Members may request that personal information not be passed onto a third party. However, this will result in the member being unable to receive mailings. A member may request, at any time, a copy of personal information held by the ACPPM.*

### **15. Application to Employee Records**

- 15.1 The handling of employee records will be in accordance with workplace relations legislation. This Privacy Policy will apply to protect records not covered by other legislation.
- 15.2 Employee records will not be used for commercial purposes unrelated to the employment context.
- 15.3 Any offer of employment is confidential between the employee and the ACPPM. Salary details are confidential.

- 15.4 Employment conditions (including details of salary packages) may be discussed by senior staff, Executive Committee and Council (as appropriate).
- 15.5 Staff who in the course of their employment have access to details of employment related information, including details of salaries, in a planning and management role, in the preparation of pay and associated paperwork, or in the case of network administration, while recovering electronic files or conducting computer network administration and “housekeeping”, must keep this information confidential. Particular care should be taken by staff with printing or copying employment related or sensitive material to ensure that information is not incorrectly circulated or inappropriately made available to a third party. If a document, spreadsheet or other information is sighted or handled, it should not be copied or read other than for a specific and valid work related reason and the content must not be disclosed.
- 15.6 Under no circumstances are details of salary or employment conditions to be advised to a third party other than in accordance with paragraph 5.1. Every request must be referred to the CEO or an appropriate delegate. Material relating to salary or employment conditions must not be copied or retained other than for specific work-related reasons.
- 15.7 An individual may seek written confirmation of their employment or salary (such as to support an application to a financial organisation, a loan application or similar). Release of information must be:
  - 15.7.1 agreed by the individual; and
  - 15.7.2 in accordance with paragraph 5.1; and
  - 15.7.3 at an appropriate level, such as the CEO or delegate.
- 15.8 A staff member seeking details of another person’s salary or employment conditions must be advised that the request is inappropriate. Provision of any information in response to such a request would be a serious breach of confidentiality.
- 15.9 The name, work telephone contact, e-mail and work address details of staff may be published on the ACPPM’s web page, in material produced by the ACPPM and in directories and information produced for the use of staff and those responsible for the management and governance of the ACPPM. Home or residential address and telephone details will be restricted to circulation within the organisation.

## **16. E-mail and Internet Access and Use**

- 16.1 When Internet access or e-mail are made available by ACPPM, use is to be for business purposes only. Usage patterns may be monitored. Access to e-mail or the Internet is expected to be conservative in use.
- 16.2 Sites visited by a user on a ACPPM account or network may be recorded or logged including the logging of Internet use by user name and time spent on particular sites.
- 16.3 Under no circumstances should sites containing offensive material be accessed nor should such material be downloaded. "Offensive" mean images or text that is not acceptable for general viewing and includes material of a sexual, ethnic, racial or religious nature that may cause offence to others.
- 16.4 When an e-mail box is provided, the allocation of a personal e-mail address does not imply ownership of correspondence to or from that e-mail box. Any correspondence to or from an e-mail box on the ACPPM domain or through a ACPPM provided service should be regarded as business correspondence. ACPPM retains ownership of all correspondence.
- 16.5 E-mail is normally transmitted within the ACPPM domain without intervention and without being sighted by anyone other than the addressee. However, e-mail may be intercepted by the network administrator and may be read by others. Privacy of e-mail is not guaranteed.

Copies of e-mail (including e-mail deleted by the recipient) may be saved or logged, including in the backup process, and may be viewed or read by network administrators or managers.

- 16.6 E-mail should be regarded in the same way as written correspondence and must be filed, subject to privacy considerations. E-mail should be regarded as a form of written correspondence.
- 16.7 External e-mail is transmitted over the Internet and is not secure.
- 16.8 "Junk" or "spam" e-mails should never be forwarded, nor should jokes or attachments such as graphics, illustrations, photos or executable files, other than for business related purposes. E-mail must not be used to harass, flame (to send abuse), defame, disclose information without authority, or to transmit pornography or offensive material.

## **17. Contact**

- 17.1 The contact for matters related to this privacy policy is the CEO.

*End of Privacy Policy*