

# Asbestos Disease Support Society

## PRIVACY POLICY

### Purpose

The Asbestos Disease Support Society Limited (the 'Society'), is a charitable organisation registered with the Australian Charities and Not-For-Profits Commission and provides services to people who have been diagnosed with an asbestos related disease, their family and carers. In providing services, staff of the Society work within a Code of Conduct to provide services that are valued, promote privacy, dignity, self-esteem and independence of our members.

The purpose of this policy is to provide clear guidelines on the collection, access and use of members' personal information.

### Scope

This policy applies to all persons employed, student placement, volunteers and directors of the Society.

### Why do we collect Personal Information

In order to provide services, personal information is collected and used in accordance with privacy principles and applicable legislation. This information may be in electronic or paper form. Personal information held, includes information provided to us on our membership application form (which then forms part of our membership database) and individual member files that are created when we commence support to that member. Examples of other forms of personal information includes health information, circumstances relating to your request/need for Society assistance or other information voluntarily disclosed to the Society.

### Privacy Principles

The Society respects your privacy and is committed to protection of any information you provide to us or we collect on you and to being transparent with you with respect to your information. We have adopted the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988 (Cth)*. The APPs govern the way in which we collect, use, disclose, store, secure and dispose of your personal information.

A summary of the APPs is included in this document and may also be obtained from the website of The Office of the Australian Information Commissioner at [www.aoic.gov.au](http://www.aoic.gov.au)

Importantly, the Society will only disclose your personal information under the following circumstances:

- Where you consent to the use or disclosure; and
- Where required or authorised by law.

## Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information. The Society also adopts the position that your relationship circumstances is also of a sensitive nature.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained
- With your consent or where required or authorised by law.

## Security of Personal Information

Your personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification or disclosure. Access is limited to those who require access to carry out their role.

When your personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your personal information. However, most of the personal information is or will be stored in client files which will be kept by us for a minimum of 7 years.

## Access to your Personal Information

You may access your personal information we hold about you and to update and/or correct it. If you wish to access your personal information, please contact the Society at [inquiries@adss.org.au](mailto:inquiries@adss.org.au)

In order to protect your personal information we may require identification from you before releasing the requested information.

## Complaints

If you believe your information has been inappropriately collected or managed, you can contact the General Manager and ask for your complaint to be investigated. All complaints are managed under the Society's "Complaints Policy and Procedures", which is located on the website at: XXXXX or we can send you a copy upon request. We aim to investigate and provide you with the written outcome of the investigation within 21 days of receipt of the complaint.

If you are dissatisfied with the investigation, you can complain to the independent Australian Information and Privacy Commissioner. The Australian Information and Privacy Commissioner has the power to investigate complaints about possible breaches of the *Privacy Act 1988*, order compensation to be paid and order agencies to change the way they handle personal information where it is not being done according to law.

While it is possible for the first contact to be with the Australian Information and Privacy Commissioner, the Commissioner's office will usually always ask the organisation to conduct its own inquiry first and provide the findings. It is therefore more timely for you to contact the Society as the first step should you hold concerns about your information.

## Summary of Australian Privacy Principles (APP)

### APP 1: Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

### APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

### APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

### APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

### APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

### APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

### APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

### APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

### APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

#### APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

#### APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

#### APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

#### APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

## Summary of National Privacy Principles (NPP)

### NPP 1 – Collection

Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection that the person can get access to their personal information and what happens if the person does not give the information.

### NPP 2 – Use & Disclosure

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

### NPP 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.

## Asbestos Disease Support Society

### **NPP 4 – Data Security**

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

### **NPP 5 – Openness**

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

### **NPP 6 – Access & Correction**

Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.

### **NPP 7 – Identifiers**

Generally speaking, an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government ‘agency’.

### **NPP 8 – Anonymity**

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do.

### **NPP 9 – Transborder Data Flows**

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

### **NPP 10 – Sensitive Information**

An organisation must not collect sensitive information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety).

Members wishing to access the personal information should put their request to the General Manager at [inquiries@silicosissupport.org.au](mailto:inquiries@silicosissupport.org.au)