Privacy Policy

1. Purpose

1.1 This Privacy Policy (the Policy) establishes the principles and approach to ensure compliance with Federal and State/Territory based Privacy Legislation regarding the collection, use, disclosure, storage, security and access to the personal information of clients, donors, members, volunteers, job applicants and staff.

2. Commencement of the Policy

2.1 This Policy will commence from 1 March 2017. It replaces all other Privacy policies of Arthritis & Osteoporosis New South Wales (AONSW).

3. Application of the Policy

3.1 This Policy applies to all activities of AONSW from the date of commencement.

3.2 AONSW Privacy Policy will be made publically available in both a long and short version.

3.3 A shortened version of the Privacy Policy will be provided to individuals when registering for membership or services.

4. Definitions

4.1 **Australian Privacy Principles (APPs):** principles pertaining to the handling of personal information as set out in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Reform Act).

4.2 **Member:** A person whose name is entered in the register as a member AONSW (includes paid memberships and Honorary Life Memberships).

4.3 **Donor:** A person who donates money to support the work of AONSW, including: regular giving, one-off donations, major donations, and bequests.

4.4 **Sponsor**: A person or organisation who receives set benefits through providing money or products to support events of AONSW.

4.5 **Personal Information:** Defined by the Privacy Act as “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.”

4.6 **Sensitive Information:** A subset of ‘personal information’ defined in s6(1) of the Privacy Act to mean information or an opinion about an individual’s:

a) Racial or ethnic origin
b) Political opinions
c) Membership of a political association

d) Religious beliefs or affiliations
e) Philosophical beliefs
f) Membership of a professional or trade association
g) Membership of a trade union
h) Sexual preference or practices, or
i) Criminal records
j) Health information, genetic information or biometric information about an individual

4.7 Health Information: A type of personal and sensitive information including information or opinion about matters such as:

a) Mental health
b) Disability
c) Health preferences
d) Use of health services
e) Bodily donations
f) Genetic information
g) Personal information collected to provide, or in providing a health service,
h) Healthcare identifiers

4.8 **De-identified Information:** Information no longer about an identifiable individual or an individual who is reasonably identifiable.

4.9 **Frivolous or vexatious:** An act which is not undertaken in good faith, but intended to annoy or embarrass another party, or when it is not calculated to lead to any practical result.

4.10 **Notifiable Data Breaches (NDB) Scheme:** Part IIIC of the Privacy Act that requires organisations to notify individuals and the Commissioner of eligible data breaches.

4.11 **Serious harm:** Access, disclosure or loss of a persons information that may inc lude serious physical, psychological, emotional, economic and financial harm, together with serious harm to reputation. Serious harm is determined through reviewing the following factors, in relation to the access, disclosure or loss of a persons information:

- the kind/s and sensitivity of the information;
- if the information is protected by security measures (e.g. by a password);
- the persons or kinds of person who have obtained or could obtain the information; and
- the nature of the harm.

4.10 **Eligible data breaches**: Unauthorised access to, unauthorised disclosure of, or loss of, personal information that a reasonable person would conclude the access, disclosure or loss that has been determined to be likely to result in serious harm to the individual/s to whom the personal information relates.

4.12 **Notification Statement:** A statement that is used when an eligible data breach occurs or is suspected. The statement must contain the following information:

- the name and contact details of the organisation/s;
- a description of the breach;
- the kind(s) of information impacted by the breach; and
- recommendations about the steps affected individuals should take in response to the breach.

4.13 **Commissioner:** The Australian Information Commissioner that is informed if an eligible data breach occurs and if aware of a breach by an organisation can direct them to complete a Notification Statement.
4.11

5. Privacy Laws

"Personal", "Sensitive" or "Health" Information

5.1 In collecting "personal", "sensitive" or "health" information, AONSW is bound by the Privacy Act 1988, and the Australian Privacy Principles (APPs) therein, in addition to applicable state legislation.

6. Type of Personal Information Collected

6.1 AONSW will only collect personal information which is reasonably necessary to deliver our services or conduct business activities and functions of the organisation.

6.2 Types of information collected:

Personal Information

a) Personal information relevant to the individual's relationship with AONSW, including a person's name, address, date of birth, contact details, next of kin or emergency contact, gender, languages and payment details.

b) Where practical and requested, individuals may be allowed to remain anonymous or to use a pseudonym in accordance with APP

Sensitive Information

a) Sensitive information may be collected regarding racial or ethnic origin, religion, membership of a professional trade or association, sexual preference, criminal records, with express or implied consent,

b) Health Information,

c) Health information relating to provision of information or services, such as diagnoses, treatments, disabilities, reports, healthcare identifiers, pharmaceuticals.

7. Method for Collecting and Holding Personal Information

7.1 Personal information collected may be verbal, written, audio, video, electronic or photographic.

Source of Information

7.2 Where possible, personal information will be collected directly from the individual concerned or their authorised representative. Methods may include:

a) Electronic interactions eg website, mobile phone
b) Face to face interviews
c) Forms and written requests for information
d) Provision of goods and services

7.3 Information may also be collected through

a) Referrals from other service providers
b) Donations and campaigns
c) Commercial list providers or information shared with other charities

Notification

7.4 When collecting personal information, AONSW will provide individuals with a short privacy notice before or shortly after collection outlining:

a) The organisation's identity and contact details.
b) The fact that information has been collected, if gathered from a third party or if the person is unaware.
c) Whether the collection of information is authorised or required by law (eg APP).
d) The purposes for which the information is collected.
e) The main consequence if the (health) information is not collected.
f) Any other persons or entity to which the information may be disclosed.
g) That AONSW privacy policy explains how they can access and correct information held about them.
h) That AONSW privacy policy explains how to make a complaint about a breach of the APPs.
i) Whether the information is likely to be disclosed to overseas recipients, and if so, in which countries.

Consent

7.5 Wherever practical, individual consent will be obtained before collecting, storing or disclosing personal, sensitive or health information.

7.6 Consent must be fully informed and voluntary.

7.7 Methods of consent may include:

a) Signature (preferred)
b) Verbal - documented, recorded or otherwise
c) Email
d) Implied consent is to be used cautiously. This may include situations where an individual contacts AONSW and provides information; leaves voice recorded phone message; or does not select an opt-out option provided.

Financial Transactions

7.8 AONSW applies additional security measures to ensure security of your financial information.

a) Where required, AONSW may store credit card details on its computer systems in an encrypted format.

b) Credit Card information and transaction security is protected through use of encryption software. This means that all personal information, including name, address and credit card number, cannot be read as a transaction travels across the internet from your computer to AONSW computers, or from the AONSW computers to a bank.

c) Payment forms or other hard copy financial information is stored in locked filing cabinets and only accessible by authorised staff members.

Permitted Situations

7.9 **Sensitive and health information** will only be collected, used or disclosed with the individual's consent, with the exception of "permitted situations" addressed in section 10.

7.10 Standard consent forms will be used for people attending camps or direct services, where AONSW may be required to disclose information to health services or contact ambulance in an emergency.

Website

7.11 AONSW may collect anonymous information about visitors to our website and their activity in order to improve the website and services.

7.12 Information collected may include the date, time and duration of visits; which pages are commonly visited; referral sites.

7.13 AONSW website may use 'cookies' – small files stored on the user's computer to hold modest amount of data specific to a particular individual and website.

a) Cookies can be accessed via the web server or the client computer.
b) Cookies may be used by the server to tailor a page to a particular user.
c) A webpage may access data in the cookie to carry information from one visit to the website to the next.
d) Cookies may also manage security and store information about the type of browser being used.
e) Most internet browsers enable users to erase or block cookies, or receive notification before one is installed on their computer. However, some functions on the AONSW website may be impacted if cookies are disallowed.

Storage

7.14 AONSW takes reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure through the following security measures:

a) Staff and volunteers who have access to personal information are required to sign confidentiality and privacy clauses in agreements.

b) Electronic storage in secure databases, held within Australia.

c) Computer and network security is maintained through use of firewalls (security measures for the Internet) and other security systems such as user identifiers and passwords to control access to our computer system.

d) Hard copies of personal information, where required, are stored in locked filing cabinets and AONSW premises are protected with security systems.

e) Secure waste bins are utilised on premises for secure and timely disposal of personal information not required.

f) Archiving of hard copy material is outsourced to a supplier compliant with privacy legislation, and retention dates are recorded. Information will generally be kept for 7 years, for adults accessing direct services. In the case of children, records will be kept until the individual reaches 25 years of age.

g) Where personal information is no longer required by AONSW, or required by law, AONSW will take reasonable steps to destroy or de-identify information in accordance with legal requirements for retention and disposal.

8. Use of Personal Information

8.1 Personal information will only be used for the primary purpose for which it is collected, unless the individual consents for the information to be used for another purpose.

8.2 Access to member, consumer and donor information will be controlled on a need to know basis through database permission controls.

8.3 AONSW will not use an individual's government identifiers as our own identifier of the individual.

Members

8.4 The primary use of member information is defined by the objectives and purposes of the company constitution:

a) Contribute to the development of a centre of excellence in musculoskeletal health.

b) Support people living with arthritis and associated musculoskeletal conditions by providing up to date evidence based information, education and services.

c) Contribute to, and promote research into the causes and treatment of arthritis and associated musculoskeletal conditions.

d) Create, administer and assist a network of support groups and branches across NSW.

e) Advocate for the development of policies and programs with government and non-government organisations which aim to promote quality of life for people with arthritis and other associated musculoskeletal conditions.

f) Grow the AONSW brand and achieve regular and sustained income within the legal guidelines.

8.5 Communications regarding marketing, fundraising, bequests and donations will include a simple option to opt-out.

8.6 Express permission will be requested before Member information is shared with branches and other members.

Non-Members

8.7 For non-members, the primary use of personal information may be confined to one or more of the above purposes, including the following functions:

a) Fundraising
b) Sponsorship
c) Donations
d) Bequests
e) Services
f) Information and events
g) Research

8.8 Where AONSW uses personal information to contact non-members for purposes other than their primary reason for contact (eg fundraising), individuals will be provided with an easy option to opt-out of this and future such communications.

8.9 Donors will be provided with a choice to opt-out on future communication regarding fundraising activities or new campaigns.

Quality of Information

8.10 AONSW will take reasonable steps to ensure personal information collected, used or disclosed is accurate, up-to-date, complete and relevant.

8.11 If information is found to be inaccurate, out of date, incomplete, irrelevant or misleading, steps will be taken to correct the information and communicate these changes to parties in receipt of such information.

9. Access to Personal Information

9.1 Individuals will be supported to access, correct or modify information held about them by AONSW on request, unless the following apply:

a) Providing access could pose a serious threat to the life, health or safety of an individual or the public.

b) Providing access would have an unreasonable impact on the privacy of other individuals.

c) The request is frivolous or vexatious.

d) Information relates to existing or anticipated court proceedings and would not be accessible by discovery in those proceedings.

e) Giving access would be unlawful.

f) Denying access is required or authorised by Australian law or a court/tribunal order.

g) Giving access would prejudice the organisation taking appropriate action where the organisation suspects unlawful activity or serious misconduct that relates to its functions or activities.

h) Giving access would reveal evaluative information generated within the organisation in connection with a sensitive decision making process.

10. Permitted Situations

10.1 Sensitive and Health information may *only* be collected, used or disclosed without consent where the information:

a) Relates to the activities, purposes or objects of AONSW, and

b) Relates solely to members of AONSW or to individuals who have regular contact with the organisation in connection with its activities, and

c) It is unreasonable or impractical to obtain the individual's consent, and

d) It is reasonably believed to be necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to the public health or safety, or

e) There is reason to suspect that unlawful activity or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, or

f) It is reasonably necessary for a legal or confidential alternative dispute resolution process.

11. Disclosure of Information

11.1 Personal information will only be disclosed for the primary purpose for which it is collected, unless the individual consents for the information to be used for another purpose.

11.2 Health Information may be disclosed to an immediate family member for compassionate reasons when this is not contrary to express wishes of the individual.

Third Party Marketing

11.3 Personal information will not be disclosed to another party (eg NFP) for purposes of direct marketing, without the individual's consent.

Trans-border Flow of Information

11.4 AONSW endeavours to utilise suppliers located in Australia to avoid the need for trans-border flow of information.

11.5 In the event that it is necessary to transfer information overseas (eg if local services are unavailable or cost prohibitive, or for individual health needs), AONSW would take reasonable steps to ensure that any overseas recipient or supplier is subject to similar privacy protection laws as Australia.

Miscellaneous

11.6 Furthermore, AONSW will not disclose the following information without consent:

a) Details about an adopted person, birth parent or adoptive parent.
b) Details about a person with a spent or extinguished conviction.
c) That a person is subject to a forensic investigation in relation to a crime or their DNA information.

12. 12. Eligible Data Breach Reporting

12.1 All suspected eligible data breaches are to have an immediate assessment and if there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach, the Chief Executive Officer must report it to the Commissioner within 30 days of the suspicion of the breach using the Notifiable Data Breach Form at https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

12.2 If an eligible data breach has occurred the Chief Executive Officer must be report it using a the Notifiable Data Breach Form at https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB as soon as practicable and all individuals are to be informed of the breach and the information contained in the Notification Statement. If this is not practical, the Notification Statement is to be published on AONSW's website and to be publicised.

13. Workplace Surveillance

13.1 As per the AONSW Internet, Email and Computer Use Policy, individuals who use AONSW computers may be subject to computer surveillance at such times of AONSW choosing and

without further notice to any user.

13.2 AONSW will give at least 14 days' notice if conducting camera surveillance or tracking devices in the work place.

13.3 Surveillance cameras in the workplace or on vehicles will be visible, with appropriate signage.

13.4 AONSW will not engage in prohibited surveillance, such as, when an employee is not at work, or in locations such as change rooms or toilet facilities.

14. Complaints

14.1 Complaints and concerns about AONSW application of the APPs or relevant privacy laws can be referred to the AONSW Privacy Officer.

14.2 Complaints may be made in writing, via email, phone or in person.

14.3 The Privacy Officer will consider the complaint and work with the complainant towards a satisfactory resolution.

14.4 AONSW will generally respond to a privacy complaint within a week, and will endeavour to complete the investigation and resolution within 30 days of receipt. In complex cases, the time-frame may be longer.

14.5 Individuals making a complaint will not be disadvantaged as a result.

14.6 If you are not satisfied with our response to your complaint, you are entitled to make a complaint to the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner can be contacted by telephone on 1300 363 992. Full contact details for the Office of the Australian Information Commissioner can be found online at www.oaic.gov.au.

Variations

AONSW *reserves the right to vary, replace or terminate this policy from time to time*.

Associated documents

- Constitution of Arthritis NSW
- Computer Use Policy
- Confidentiality Agreement
- Code of Conduct
- Employee contract/HR policies
- Privacy Statement (short version)
- Social Media Policy

Associated Legislation

Privacy Laws including:

- *Privacy Act 1988* (Cth) (**Privacy Act**) from 12 March 2014, sets out the Australian Privacy Principles (**APPs**)
- Privacy Amendment (Notifiable Data Breaches) Bill 2016
- *Privacy and Personal Information Protection Act 1998* (NSW), which sets out the Information Protection Principles (**NSW IPPS**), and *Health Records and Information Privacy Act 2002* (NSW) which sets out the Health Privacy Principles (**NSW HPPS**)
- *Health Privacy Principles* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *ACT Information Privacy Act 2014*

- Other state and territory health and information privacy legislation if applicable

Reference Documents

- Privacy Guide: A Guide to compliance with New South Wales and Federal privacy laws. Justice Connect, 22 April 2015
- Australian Government Office of the Information Commissioner (AOIC) https://www.oaic.gov.au

Policy version and revision information

Action	By whom	Version	Date
Created	Helen Wilson Consultancy		
Approved	CEO	V1.0	03.02.17
Reviewed by	Governance Committee	V1.0	02.05.17
Review	CEO		01.03.18
Review	Business Development and Engagement Manager	V1.1	20.02.18
Approved	Board	V2.10	15.05.18