CPSA COMBINED PENSIONERS & SUPERANNUANTS ASSOCIATION OF NSW INC

PRIVACY

1.0 STATEMENT

Combined Pensioners & Superannuants Association of NSW Inc (CPSA) is committed to ensuring that each individual's right to privacy and confidentiality is respected and protected in accordance with law, and that confidential organisational documents are protected.

2.0 SCOPE

The scope of this procedure has application for all activities and personnel involved with the collection, storage, use and disclosure of both personal and corporate information relating to non-employees.

3.0 DEFINITIONS

Personal Information is defined under the Freedom of Information Act Section 4 to mean information or an opinion . . . about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, regardless of whether that information is true or not.

Sensitive Information means any information about a person's individual preferences, race, religion, political opinions, affiliations, philosophy, membership, health, genetics, criminal record, biometric information / templates for the purpose of automated biometric verification / identification.

Where definitions are unclear, refer to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* and Schedules.

APP is Australian Privacy Principle(s).

4.0 OBJECTIVE

CPSA will ensure that any process for the collection, storage, use or disclosure of personal information will comply with applicable privacy laws and regulations, specifically the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*. These obligations cover:

1. open and transparent management of personal information
2. anonymity and pseudonymity
3. collection of solicited personal information
4. dealing with unsolicited personal information
5. notification of the collection of personal information
6. use and disclosure of personal information
7. direct marketing
8. cross-border disclosures
9. adoption, use or disclosure of government related identifiers
10. quality of personal information

11. security of personal information
12. access to personal information
13. correction of personal information

5.0 PROTOCOL

5.1 APP 1: open and transparent management of personal information

5.1.1 The kinds of personal information CPSA collects

CPSA collects personal information only when necessary for one or more CPSA functions or activities, such as providing membership benefits, systemic advocacy or individual casework assistance. Generally this includes contact details only. Individuals may interact with CPSA anonymously when seeking advice or information and CPSA will provide generalist advice on this basis. However, for more details casework, CPSA may be required to collect details specific to the case which will assist in achieving a positive outcome for the individual client.

CPSA may collect and collate opt-in de-identified personal information through Member surveys, in order to assist with systemic advocacy and achieve positive outcomes for CPSA constituents generally.

5.1.2 How CPSA collects personal information

Information will be collected in a fair and reasonably unobtrusive manner, such as when freely provided over the phone, in writing or which is publicly available. Where possible, information is collected only from the individual concerned or their legal guardian, representative or advocate. When the purpose of collection is not immediately clear (ie if it is not being provided for a specific purpose already discussed), CPSA will inform individuals the purposes for which the information is collected, and any third party to which the information would normally be disseminated.

5.1.3 Accessing the CPSA Privacy Protocol

The CPSA Privacy Protocol will be made freely available on the CPSA website and via contacting CPSA Head Office, and a notice to this effect will be placed in *THE VOICE,* so that all Members are aware of its existence and means of access.

5.1.4 How an individual may complain about a breach of the APPs

An individual may complain about a breach of the APPs using the complaints mechanism of the CPSA Constitution.

5.2 APP2: Anonymity and pseudonymity

When seeking advice or information, individuals may interact with CPSA anonymously where practicable for CPSA and where allowable by law and CPSA will provide generalist advice on this basis. However, for more detailed casework or where it is impracticable to deal with individuals who have not identified themselves, CPSA may be required to collect

details specific to the case which will assist in achieving a positive outcome for the individual client, or for CPSA's activities and functions.

CPSA membership is contingent on provision of correct contact details as required by NSW Associations Incorporation Act (2009) and Regulations (2010).

5.3 APP3: Collection of solicited personal information

CPSA will not collect personal or sensitive information except with the individual's consent and only when reasonably necessary to advance CPSA advocacy or casework for a more positive outcome for the individual. It may be collected in person, over the phone, or in writing.

Sensitive information will not be collected unless it is unreasonable or impracticable to exclude it or under APP6.

5.4 APP4: Dealing with unsolicited personal information

If unsolicited personal information is provided, the recipient will determine whether collection would have been permitted under APP 3. If so, APPs 5 – 13 apply. If not, the unsolicited personal information will be destroyed or de-identified where possible, except where destruction or de-identification is unlawful or unreasonable (eg would compromise legitimate information which will assist CPSA in its aims and objectives).

5.5 APP5: Notification of the collection of personal information

CPSA will notify individuals on the CPSA website and through *THE VOICE* (sent to all Members) of the existence of this Protocol, and therefore information about access, correction, overseas dissemination and complaints processes relating to individuals' information.

If personal information has been collected from a third party, or if the individual is likely unaware that the information has been collected, CPSA will take reasonable steps to ensure that an individual is notified what and how that information is usually (or has been) collected.

5.6 APP6: Use and disclosure of personal information

CPSA will only use or disclose personal information to achieve the purpose for which it was provided, except where:

- the individual has consented to use or disclosure; or
- use or disclosure is both relevant and reasonably necessary, such as:
  - Where required by law;
  - To assist in locating a missing person;
  - To lessen or prevent a serious threat to the individual or the public (consent will be sought where reasonable and practicable);

- ❖ To investigate or relevantly report a suspicion of unlawful CPSA-related activity;
- ❖ To an enforcement body for enforcement related activities;
- ❖ To establish, exercise or defend a legal or equitable claim; or
- ❖ For the purposes of a confidential alternative dispute resolution.

5.7 APP7: Direct marketing

CPSA will not use or disclose personal information for direct marketing purposes. CPSA may use personal information to remind individuals of membership benefits or CPSA services, for overdue membership fees or the like, and this may include options to make donations to CPSA. Personal information will not be provided to a third party for this purpose.

5.8 APP8: Cross-border disclosures

CPSA will not disclose information to overseas recipients except in accordance with APP 6. Any act or practice by the overseas recipient which breaches the APPS may be taken to be a breach by CPSA. CPSA works in the cloud, and all cloud-based work is password protected. Any real or suspected breach of data will be informed to Members if reasonable and practicable.

5.9 APP9: Adoption, use or disclosure of government related identifiers

CPSA does not adopt, use or disclose Government-related identifiers (eg Pension Card number, Medicare number, Tax File Number), except:

- ➢ as reasonably necessary to identify the individual for the purposes of CPSA activities or functions (eg to confirm that an individual is a pensioner, for either casework or other benefit to the individual);
- ➢ as necessary to fulfil obligations to the issuing agency;
- ➢ as permitted by law; or
- ➢ where use or disclosure is reasonably necessary for an enforcement related activity conducted by or on behalf of an enforcement body.

5.10 APP10: Quality of personal information

CPSA endeavours to ensure that personal information provided is accurate, up-to-date and complete, such as through confirming correct addresses of returned mail by public registers or telephoning the individual where possible. In addition, CPSA takes reasonable steps to ensure that personal information is relevant to the purpose of its use or disclosure.

5.11 APP11: Security of personal information

In addition to staff's familiarity with the APPs and CPSA's Privacy Protocol, CPSA protects personal information from misuse, loss, unauthorised access / modification / disclosure in the following manner:

Storage method	**Security**

Membership / contact database	Password-protected access; Individual logins provided to relevant staff only; Access and amendments are tracked; Only accessible from CPSA office or via secure VPN to CPSA office.
Membership records	Lockable filing cabinet
Individual correspondence (paper)	Lockable filing cabinet
Individual correspondence (scanned)	Password-protected
Email messages	Password-protected; Circulated only to relevant staff

Personal information (hardcopy) is stored for a minimum of seven years and before secure destruction. Certain information will be kept longer than seven years if it is legally required or is likely useful for future benefit to CPSA constituents through advocacy or individual casework. Emails may be destroyed earlier if reasonably required, such as storage constraints or ongoing irrelevance.

5.12 APP12: Access to personal information

Individuals can access their personal information for free, by appointment. Generally, an appointment can be within 5 working days of making the request, except in the absence of those CPSA staff authorised to access the information. Copies of the information are available at cost by hardcopy or scans where reasonable. If access cannot be given, CPSA will provide in writing the reasons for refusal and the mechanisms to complain about the refusal (see the complaints mechanism of the CPSA Constitution). Examples of acceptable reasons for refusal include where access may:

- Pose a serious threat to the life or health of any individual;
- Pose a serious threat to public health or safety;
- Be required or authorised by or under law;
- Likely prejudice an investigation of possible unlawful activity;
- Likely prejudice actions by or on behalf of an enforcement body in relation to unlawful activity or improper conduct; or
- Affect current, past or future suspected unlawful activity or serious misconduct relating to CPSA functions or activities, or prejudice CPSA or an enforcement agency taking appropriate action or enforcement related activities in relation thereto.

If CPSA declines to provide access to personal information, CPSA will:

- Notify the individual in writing:
  - the reasons for refusal unless the reasons make it unreasonable to do so;

- ❖ the complaint mechanisms available (as outlined in the CPSA Constitution); and
- ❖ any other matters prescribed by the regulations; and

- ➢ endeavour to provide access in a mutually satisfactory manner, such as through a mutually agreed intermediary.

5.13 APP13: Correction of personal information

To ensure that personal information is up-to-date, complete, relevant and not misleading, CPSA will correct (as promptly as practical), without cost to the individual, personal information for the purpose for which it is held if:

- ➢ CPSA is satisfied that it needs to be corrected; or
- ➢ The individual requests that it be corrected.

If CPSA declines to correct any information, CPSA will provide notice in writing in accordance with APP 12.

If the individual requests that a note be attached to the information confirming its accuracy, and this accords with CPSA's review of the information, a note will be attached.

If the individual so requests, CPSA will notify this update to other APP entities which have been provided with the personal information.

6.0 CPSA Practices

6.1 Commitment to Confidentiality

Protecting information is a significant responsibility. CPSA, as an organisation that holds information about individual people has a duty to handle that information responsibly.

CPSA aims to use this information appropriately and to give assurances and guarantees that such information will be kept in a confidential and safe manner and will only be used for the achievement of the goals of CPSA. However, the individual or organisation's right to privacy is not absolute. Information will be released in accordance with legal requirements and the CPSA Constitution.

All members of the Management Committee and all employees and contractors of CPSA must affirm their commitment to maintaining confidentiality in relation to all CPSA's business affairs, through the signing of the Code of Conduct and Ethics.

All records of personal information are to be stored in a protected environment.

The *Records Register* identifies where each type of confidential record is stored, who is responsible for it, what protections are in place, and the period files are to be maintained in archives before being destroyed, in accordance with legislative timeframe requirements.

6.2 Privacy Protection - General

Control over the movement of information is of the utmost importance. No information should be removed or copied without a tracer note stating date, destination and reason for the information's removal or duplication. Staff are not authorised to talk to outside

agencies about any matters relating to finances, internal issues of CPSA, their grant, or any other grant without prior permission of the CPSA General Manager.

6.3 Privacy Protection – Core Files

Core files are stored in the compactus. Client files and any documents of a sensitive nature, such as relating to complaints, disputes or insurance claims as stored in lockable filing cabinets.

Staff may access their own personnel files that are maintained by the CPSA Accountant and Administration Coordinator. On request (written or verbal), a staff member will be presented with their current file. The cabinet will remain locked while they review it under supervision of the CPSA Accountant or Administration Coordinator (to ensure that records are not tampered with). Any changes that the staff member wishes to make must be presented to the General Manager in writing.

6.4 CPSA Staff Responsibilities

The General Manager is accountable and responsible to the CPSA Executive for all matters and concerns about Privacy within CPSA and will monitor and review the procedures for privacy at regular time periods.

It is the responsibility of all CPSA staff to:

- Take reasonable care and follow correct procedure with regard to privacy
- Seek any clarification about procedures/protocol concerning privacy from the General Manager as soon as possible
- Co-operate with the General Manager if any breaches or misunderstandings have occurred about privacy issues/procedures within this organisation

Staff must also ensure that individual interviews or consultations conducted with Members at CPSA premises take place in a suitable area, with sight and sound privacy.

Co-ordinators are to ensure that any personal interviews conducted with their staff are also undertaken in a suitable area, where confidential discussions cannot be overheard.

6.5 Breach of Standards

Any breach of procedure or ambiguity concerning protocols about privacy issues in this organisation should be immediately reported to the General Manager.

For more information, the Privacy Commissioner's Office Sydney on 02 8019 1600.