Privacy, Confidentiality and Consent Policy

Policy number:	013	Version:	20260103
Drafted by:	G. Harrison	Approved by Committee on:	
Responsible person:	Privacy Officer	Scheduled review date:	03 Feb 2027

1. Purpose

Veterans' Centre Mid North Coast Inc. (t/a Veterans' Wellbeing Network Mid North Coast) (herein after the "Network") is committed to protecting the privacy, dignity, confidentiality and security of all veterans, families, members, volunteers and stakeholders.

This policy establishes the requirements for the collection, storage, use, disclosure, retention and destruction of personal and health information obtained by the Network while providing advocacy, welfare, wellbeing and support services.

The Network recognises that information relating to veterans frequently contains sensitive personal and health information, including Department of Veterans' Affairs (DVA) records, medical reports, psychiatric assessments, compensation claims and family information, which require a high level of protection. [The Privacy Act | OAIC], [Guide to health privacy]

2. Legislative Framework

This policy is intended to support compliance with:

- Privacy Act 1988 (Cth).
- Australian Privacy Principles (APPs).
- Notifiable Data Breaches Scheme.
- Health Records and Information Privacy Act 2002 (NSW).
- Privacy and Personal Information Protection Act 1998 (NSW).
- ACNC Governance Standards.
- Relevant DVA requirements and authorisations. [Privacy Act 1988 - Federal Register of Legislation]

3. Scope

This policy applies to:

- Committee members,
- Volunteers,
- Advocates,
- Wellbeing Support Officers,
- Employees,
- Contractors,
- Consultants, and
- Any person authorised to access Network records.

4. Privacy Principles

The Network will:

- Collect only information necessary to provide services.
- Obtain informed consent wherever practicable.
- Use information only for authorised purposes.
- Protect information from misuse, loss and unauthorised access.
- Allow individuals access to their information.
- Correct inaccurate information when required.
- Destroy or de-identify records when no longer required.
- Respond promptly to privacy complaints and incidents. [legislation.gov.au], [oaic.gov.au]

5. Information We Collect

The Network may collect Personal Information such as:

- Full name,
- Date of birth,
- Address,
- Telephone numbers,
- Email addresses,
- Emergency contacts,
- Membership records, and
- Australian Defence Force (ADF) Service history.

The Network may also collect Sensitive Information:

- Medical records,
- Mental health information,
- Psychiatric reports,
- Health assessments,
- DVA claim information,
- Compensation records,
- Rehabilitation information,
- Financial information relevant to advocacy matters, and
- Cultural background where necessary.

Sensitive information will only be collected where necessary and with appropriate consent unless otherwise authorised by law.

6. Collection of Information

The Network may collect information through:

- Membership applications,
- Interviews and consultations,
- Consent forms (Consent for Family to Act, Privacy and Consent – Veterans, etc),
- Authority to Act forms (ADF Records, DVA, etc),
- DVA correspondence,
- Medical providers,
- Referral services, and
- Email, telephone and written communication.

Information will normally be collected directly from the individual concerned.

7. Consent Requirements

Before collecting, obtaining, using or disclosing health information the Network will obtain written consent wherever practicable.

The Network will maintain:

- Consent to Collect and Use Information Forms,
- Authority to Act Forms, and
- Medical Information Release Authorities.

Individuals may withdraw consent at any time, subject to legal obligations and existing advocacy processes.

8. Authority to Act

Before representing a veteran in dealings with DVA, medical providers, government agencies or service providers, the Network must hold an appropriate written Authority to Act signed by the veteran or authorised representative.

Authority documents must be securely retained on file.

9. Use and Disclosure

Information will only be used:

- For advocacy purposes,
- Welfare and wellbeing support,
- Referral services,
- Volunteer management,
- Membership administration, and
- Legal and reporting obligations.

Information may be disclosed only with the individual's consent:

- To DVA,
- To medical practitioners,
- To legal advisers,
- To approved service providers,
- Where required by law, and
- To prevent serious risk to life, health or safety.

10. Confidentiality

All personnel must maintain strict confidentiality regarding information obtained through the Network. No person may:

- Discuss a client's affairs in public settings.
- Share information without authority.
- Access records unrelated to their duties.
- Remove records without approval.

All Committee Members, volunteers and Advocates must sign a Confidentiality Agreement before being granted access to veteran records.

11. Information Security

The Network will implement reasonable security controls to protect personal and health information. These controls may include:

- Physical Security:
    - Locked filing cabinets,
    - Restricted office access,
    - Secure disposal bins, and
    - Visitor controls.
- Electronic Security:
    - Multi-factor authentication,
    - Password-protected systems,
    - Device encryption,
    - Anti-malware protection,
    - Secure cloud storage,
    - Automatic updates,
    - Backup procedures, and
    - Role-based access controls.

Only authorised personnel may access confidential information. [oaic.gov.au], [legislation.gov.au]

12. Access and Correction

Individuals may request:

- Access to information held about them.
- Copies of records where appropriate.
- Correction of inaccurate information.

Requests should be directed to the Privacy Officer and the Network will respond within a reasonable timeframe.

13. Data Retention

The Network will retain records only for as long as necessary to fulfil operational, legal and governance requirements.

Unless otherwise required:

- Membership records – 7 years after cessation,
- Advocacy files – 7 years after closure,
- Financial records – 7 years,
- Volunteer records – 7 years after cessation,
- Incident records – 7 years, and
- Committee records – Permanent.

At the expiry of retention periods, records will be securely destroyed or de-identified.

14. Data Breaches

A privacy breach includes:

- Loss of records,
- Theft of records,
- Unauthorised access,
- Unauthorised disclosure,
- Cybersecurity incidents, and

- Accidental sharing of personal information

Any suspected privacy breach must be reported immediately to the Privacy Officer and the Privacy Officer shall:

- Contain the breach.
- Investigate the incident.
- Assess risk of harm.
- Determine notification requirements.
- Maintain a Breach Register.
- Recommend corrective actions.

Where required, affected individuals and regulators will be notified in accordance with applicable legislation.

15. Privacy Officer

The Network shall appoint a Privacy Officer.

Responsibilities include:

- Privacy compliance oversight,
- Complaint management,
- Breach management,
- Training coordination,
- Consent register management, and
- Policy reviews.

Contact Details:

Phone: 02 5621 8108

Email: compliance@vwnmnc.org.au

16. Privacy Complaints

Any person who believes their privacy has been breached may submit a complaint to the Privacy Officer. Complaints will be:

- Acknowledged promptly,
- Investigated fairly,
- Managed confidentially, and
- Responded to in writing where appropriate.

If unresolved, complainants may seek review through the Office of the Australian Information Commissioner or other appropriate authorities.

17. Training

All personnel handling personal or health information must complete privacy and confidentiality training:

- During induction,
- Annually thereafter, and
- Following any significant policy change.

Training records will be maintained by the Network.

18. Policy Review

This policy shall be reviewed:

- Annually, or
- Following major legislative changes, or
- Following a privacy breach, or
- Following significant operational changes.

19. Related Network documents:

- Policy 014 – Information Security Policy
- Form 001 – Consent to Collect and Use Information
- Form 002 – Authority to Act
- Procedure 001 – Data Breach Response Plan

Version history

Version	Date	Author	Rationale
20250109	09 Jan 2025	G. Harrison	Initial Draft
20260103	03 Jan 2026	G. Harrison	Further incorporation and update of the relevant acts in line with recent technology improvements in cyber security.