AUSTRALIAN NURSING & MIDWIFERY FEDERATION

TASMANIAN BRANCH

PRIVACY POLICY

Policy Name:	**Privacy Policy**
Original Approved:	March 2014
Review Frequency:	Three years
Amended & Re-approved:	December 2021
Next Review Due:	December 2024 (or as otherwise determined)

PURPOSE

This policy outlines the approach of The Australian Nursing and Midwifery Tasmanian Branch (ANMF) to meet its legal and ethical requirements in regard to the collection, storage and disclosure of personal information it holds in regard to its student population, staff, other clients and interaction with external organisations.

SCOPE

This policy applies to all ANMF (Tas Branch) employees, workplace representatives, members, students and elected officers.

POLICY STATEMENT

The Australian Nursing and Midwifery Tasmanian Branch (ANMF) is an organisation of employees (i.e. a trade union) registered under the Fair Work (Registered Organisations) Act 2009 and is also (via its subsidiary) an RTO. The ANMF is covered by the provisions of the Privacy Act 1988 and the Australian Privacy Principles (APPs) in relation to personal information and its collection and use; its disclosure and its security; and access to it. This Privacy Policy (Policy) should be read in conjunction with the Privacy Act, the APPs and the Health, Education and Research Centre (HERC) Privacy and Personal Information Policy.

In order to carry out its activities, the ANMF may collect personal information from, or on behalf of, members, students, potential members and potential students, and in some circumstances, former members and students, in order to provide professional and industrial services related to the profession of nursing, caring and midwifery or the employment of nurses, midwives and care staff, educational services and information such as newsletters and publications. Personal information is also collected from subscribers to the ANMF's publications.

Personal information includes all information or opinion about an individual whose identity is apparent or can reasonably be determined from the information or opinion and may include sensitive information, which is defined as information or opinion about an individual's membership of a trade union; sexual orientation; criminal record; or personal health.

1. How This Policy Applies

This Policy applies to personal information the ANMF collects from you:

- via one of our websites;
- via social media;
- via telephone;
- via email;
- via fax;
- in person; and/or
- in writing.

This Policy also applies to personal information the ANMF collects from any other third party, about you.

2. The Kinds of Information the ANMF May Collect

From time to time, you may voluntarily supply your personal information to the ANMF. The ANMF will record your e-mail address if you send us a message, subscribe to an email newsletter, or complete a form if this information is requested.

When you provide your personal information, it allows us, for example, to assist you with industrial relations and employment queries, inform you about industrial, social and political campaigns, and accept your application for membership. You may supply personal information to the ANMF by, for example, responding to a survey, filling in a meeting attendance sheet, taking part in a competition, completing a membership form, discussing your issues with a delegate, or signing up to a campaign. The ANMF only collects personal information that is necessary for the ANMF to perform its functions and/or activities.

Depending upon the circumstances you may provide to the ANMF, and the ANMF may collect, information such as, but not limited to, the following:

- your name;
- your contact details;
- your social media details (e.g. blogs, Twitter, Facebook, LinkedIn);
- your gender;
- your marital status;
- your employment details;
- your educational qualifications; and
- your inquiry or complaint details.

Some personal information is considered sensitive information and includes:

- your political opinions;

- your political party membership (if any);
- your union membership (if any);
- your racial or ethnic origin;
- your sexual orientation;
- any disabilities, illnesses or injuries you may have; and/or
- any other health information.

The Privacy Act allows the ANMF to collect sensitive information which relates solely to the ANMF's members or people who have regular contact with the ANMF if the sensitive information relates to the ANMF's activities. We will only collect sensitive information where we have received your consent to your personal information being collected, used, disclosed and stored by the ANMF in accordance with this Policy.

Where you provide information to the ANMF in relation to a job application, the personal information you provide will only be collected, held, used and disclosed for the purposes of considering your potential employment with the ANMF. Where you provide the details of referees, you confirm that you have informed the referees that you are providing their contact information to the ANMF, and they have consented to the ANMF contacting them and discussing the personal information you have provided in relation to the job application.

The ANMF will collect personal information only by lawful and fair means. We will collect personal information directly from you unless:

- you have consented to the ANMF's collection of your personal information from third parties; or
- we are legally required to do so; or
- it is unreasonable or impractical to do so.

Where we have collected personal information about you either directly or by other means as set out above, we will notify you at the time, or as soon as practicable, to ensure that you are aware of such collection and its purpose.

You can choose to interact with us anonymously or by using a pseudonym where it is lawful and practicable. For example, you may wish to participate in a blog or enquire about a particular campaign anonymously or under a pseudonym. Your decision to interact anonymously or by using a pseudonym may affect the level of services we can offer you. For example, we may not be able to assist you with a specific industrial enquiry or investigate a privacy complaint on an anonymous or pseudonymous basis. We will inform you if this is the case and let you know the options available to you.

If we receive unsolicited personal information about or relating to you and we determine that such information could have been collected in the same manner if we had solicited the information, then we will treat it in the same way as solicited personal information and in accordance with the APPs. Otherwise, if we determine that such information could not have been collected in the same manner as solicited personal information, and that information is not contained in a Commonwealth record, we will, if it is lawful and reasonable to do so, destroy the information or de-identify the information as soon as reasonably practicable.

3. The Purposes for Which Personal Information is Collected, Held, Used and Disclosed

The ANMF collects, holds, uses and discloses your personal information to:

- assist you with industrial relations and employment queries;
- inform you about industrial, social and political campaigns;
- provide services to you such as discounted or free benefits you are entitled to as a member of ANMF
- inform you about your rights at work;
- inform you about changes to legislation;
- refer you to a legal practitioner, accountant or other professional;
- improve our service delivery;
- manage our relationship with you;
- conduct surveys and research;
- provide educational services and professional development;
- conduct Union elections;
- enable a contractor engaged by the ANMF to provide bulk mail services, provided that the contractor may only use the information to give effect to the contract and may not provide the information to any third party.

4. Using your Information for Direct Marketing

You consent to our use and disclosure of your personal information for the purposes of direct marketing which may include providing you with information about events, products or services which may be of interest to you.

If you do not want us to use your personal information for direct marketing purposes, you may elect not to receive direct marketing at the time of providing your personal information.

5. Unsubscribing and Opting Out

If you do not wish to receive direct marketing or other communications, or a particular communication, you may request to cancel such communication(s) by:

- unsubscribing to an email newsletter at any time from the newsletter mailing list, which will unsubscribe you from all general email communication;
- 'opt out' by texting STOP in reply to a text message from ANMF;
- contacting us at any time via mail, email or telephone.

6. ANMF (Tas Branch) Websites

The ANMF's websites collect two types of information. The first type is anonymous information. The web server makes a record of your visit and logs the following information for statistical purposes:

- the user's server address;
- the user's top level domain name (e.g. com, .gov, .net, .au, etc.);
- the date and time of the visit to the site;
- the pages accessed and documents downloaded;
- the previous site visited; and
- the type of browser used.

No attempt will be made to identify users or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise a warrant to inspect the internet service provider's logs.

Another way information may be collected is through the use of "cookies". A cookie is a small text file that the website may be placed on your computer. Cookies may be used, among other things, to track the pages you have visited, to remember your preferences and to store personal information about you.

7. Security

The ANMF will take all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up to date and complete.

Personal information is kept in secured locations on the premises and is only accessed by authorised personnel. Personal information kept electronically is handled with care and secured by user identifiers, and passwords accessed only by authorised personnel. All ANMF (Tas Branch) Offices have security systems in place for the protection of all personal information stored either in paper or electronic form. An electronic backup of information is securely stored for disaster recovery purposes and is only accessed by authorised personnel.

Archived personal information is maintained in a secure offsite facility and is only accessed by authorised personnel.

Security arrangements are monitored and reviewed regularly and all staff made aware of organisational systems for the processing, storing and transmitting of personal information and the protective security policies associated with this.

8. Data Breaches

The Notifiable Data Breaches Scheme commenced on 22 February 2018. This affects breaches that occurred on or after this date.

The Notifiable Data Breaches Scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The notification must include recommendations about the steps taken in response to the breach. The Australian Information Commissioner must be notified of an Eligible Data Breach.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, that an entity holds;
2. This is likely to result in serious harm to one or more individuals; and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

Examples of data breaches that can occur are:

1. Losing a membership application form with a member's personal information on it;
2. Sending an email to the wrong recipient that includes personal information about someone, such as a member;
3. A device containing personal information is lost or stolen;
4. A database containing personal information is hacked; or
5. A Records file containing a member(s) matter is lost, stolen, or misplaced.

Where ANMF staff believe a data breach may have occurred they must immediately report the breach to the Branch Secretary (or Executive Director in the Branch Secretary's absence) who will determine the next steps in line with Appendix A – Data Breach Procedure (page 9).

9. Disclosure

The ANMF only uses or discloses personal information about an individual for the primary purpose for which the information is collected. Personal information is not used or disclosed for a secondary (related) purpose, except in accordance with the Australian Privacy Principles.

The ANMF may use or disclose personal information for a secondary purpose where the secondary purpose is related to the primary purpose of collection (or, if the personal information is sensitive information, directly related to the primary purpose), and the individual would reasonably expect us to use or disclose the information for that secondary purpose.

The ANMF may also use or disclose personal information about an individual for a secondary purpose if it has obtained the individual's consent (either express or implied).

The ANMF will not otherwise disclose personal information unless the individual has given consent or that disclosure is required by law.

No personal information is disclosed to third parties for the purposes of the third party's direct marketing.

Personal information (such as name and address) is used, from time to time, for the purpose of forwarding information in the form of member benefits, journals, newsletters

and circular letters and bulk mail management, unless an individual requests that their personal information is not used for that purpose.

The ANMF is unlikely to disclose personal information to overseas recipients. If the ANMF is likely to disclose personal information to overseas recipients, the ANMF will, if practicable, notify the individual of the countries in which the recipients are likely to be located.

Before the ANMF discloses personal information about an individual to an overseas recipient, it will take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the Australian Privacy Principles in relation to the information.

If the ANMF no longer needs personal information for any purpose for which it may be used or disclosed, and the information is not contained in a Commonwealth record and the ANMF is not required by law to retain the information, the ANMF will take reasonable steps to destroy or de-identify, the information.

10. Government Identifiers

The ANMF will not adopt as our own identifier a government related identifier of an individual, such as a tax file number or Medicare card number and will only use or disclose a government related identifier where the use or disclosure:

- is reasonably necessary for the ANMF to verify your identity for the purposes of our activities or functions;
- is reasonably necessary for the ANMF to fulfil its obligations to an agency or a State or Territory authority;
- is required or authorised by or under Australian law; or
- is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

11. Access

The ANMF will, within a reasonable period and at the written request of an individual, provide them with access to their personal information held by the ANMF. All requests by an individual for access to personal information held by us should be made in writing and addressed to ‘The Branch Secretary’ at the ANMF. The ANMF will respond to such requests within a reasonable period. There is no charge for making a request to access information but the ANMF may seek to recover reasonable costs associated with providing such access. If, for any reason, access is refused, written reasons for the refusal will be provided.

The ANMF will take reasonable steps to correct information where it is satisfied that the information it holds is inaccurate, out of date, incomplete, irrelevant or misleading, or where an individual has requested the ANMF to correct the information. All requests by an individual for correction of personal information held by us should be made in writing and directed to ‘The Branch Secretary’ at the ANMF. If, for any reason, a request for correction of such information is refused, written reasons for that refusal will be provided.

The ANMF will inform individuals when personal information is provided to an organisation providing services to the ANMF (e.g. a mailing house) when required to do so by the Australian Privacy Principles. Providers of services to the ANMF have agreed to treat all personal information provided to them by the ANMF (e.g. name and address) in accordance with the provisions of the Privacy Act and Australian Privacy Principles.

12. Complaints

All complaints about the manner in which personal information has been handled, or where access to personal information has been limited or denied, are addressed in accordance with the ANMF (Tas Branch)'s policy on Complaints.

13. Variations to the Policy

This Policy may be varied from time to time and an updated version will be posted on the ANMF (Tas Branch) websites. Please check our websites regularly to ensure that you have the most recent version of the Policy.

APPENDIX A – DATA BREACH PROCEDURE

The ANMF's first step is to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

The ANMF will consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the ANMF has reasonable grounds to believe this is the case, then it must notify individuals at likely risk of serious harm. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

The notification to affected individuals and the Commissioner must include the following information:

- the identity and contact details of the organisation

- a description of the data breach
- the kinds of information concerned and;
- recommendations about the steps individuals should take in response to the data breach.

The notification to the Commissioner can be made using the OAIC's Notifiable Data Breach form.

If ANMF only has grounds to suspect that the data breach will result in serious harm, then it must conduct an assessment process. As part of the assessment, ANMF will consider whether remedial action is possible.

If an assessment is required, ANMF will follow a four-stage process for assessment as follows:

1. Initiate: plan the assessment and assign a team or person
2. Investigate: gather relevant information about the incident to determine what has occurred
3. Evaluate: make an evidence-based decision about whether serious harm is likely
4. Document the evidence and decision

ANMF will conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, ANMF will include in the documentation why this is the case.

Where possible, ANMF will take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur. If remedial action is

successful in making serious harm no longer likely, then notification is not required, and entities can progress to the review stage.

Where serious harm is likely, ANMF will prepare a statement for the Privacy Commissioner (a form is available on the Commissioner's website) that contains:

1. ANMF's identity and contact details;
2. a description of the breach;
3. the kind(s) of information concerned; and
4. recommended steps for individuals.

ANMF will notify affected individuals and inform them of the contents in the statement via one of three options.

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the ANMF website and publicise it

When a breach requiring notification has occurred, ANMF will undertake a review and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating the security/response plan
- Considering changes to policies and procedures
- Revising/providing staff training

ANMF may also consider reporting the incident to other relevant bodies, such as:

- Police or law enforcement
- Various professional bodies
- APRA (Australian Prudential Regulation Authority) or the ATO
- The Australian Cyber Security Centre
- ANMF's financial services provider

Development and Consultation Record

Review authorised	A Brakey	Executive Director	Dec 2020
Prepared by	J Baldwin	Chief Business Officer	Feb 2021
Initial consultation with key stakeholders	Finance & Risk Management Committee		14 Dec 2021
Final consult	Branch Council		15 Dec 2021 (out of session)

Approval Record

Endorsed / Approved	Branch Council		21 Dec 2021
Additional Approval or Noting as required	E Shepherd	Branch Secretary	21 Dec 2021
Updated on N Drive	C Pond	Business Support Officer	22 Dec 2021