AMWU POLICY

PRIVACY

Introduction

The AMWU (the Union) is the union representing workers in Automotive, Food, Metals, Engineering, Printing, Technical, Supervisory and Administrative occupations registered under the Fair Work (Registered Organisations) Act 2009. The Union collects personal information in order to conduct work as a trade union. The activities of trade unionism include, but are not limited to, representing and informing workers on employment related matters as well as campaigning and lobbying on behalf of workers on matters such as industrial relations, superannuation, political economy, equality and living standards, in order to further the interests of our members and the broader community. The Union operates in the political, legal, industrial and social spheres.

The Union is committed to protecting your privacy and providing you with information and services relevant to you.

The Union complies with its obligations under the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) contained in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 which took effect on 12 March 2014. This regulates how the Union may collect, use, disclose and store personal information and how individuals may access and correct personal information held about them. This Privacy Policy should be read in conjunction with the Privacy Act and the 13 Australian Privacy Principles (APPs).

In this Policy, the Union includes the AMWU (registered as the *Automotive Food Metals Engineering Printing and Kindred Industries Union*), our National and State Branches and Divisions.

How this Policy applies

This Policy applies to personal information the Union collects from you, via one of our websites, social media, telephone, email, fax, workplace visits, in person and/or in writing.

This Policy also applies to personal information the Union collects from the Australian Council of Trade Unions (ACTU) or any other third party, about you.

What kinds of information does our Union collect?

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

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

- your name;
- your contact details;
- your social media details (e.g. Blogs, Twitter, Facebook, LinkedIn);
- your gender;
- your date of birth;

- your signature;
- your marital status;
- your employment details;
- your regular direct debit details;
- your educational qualifications; and
- your enquiry 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 religious beliefs;
- your sexual orientation;
- any disabilities, illnesses or injuries you may have; and/or
- any other health information.

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

Why do we collect it?

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 Union 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 Union only collects personal information that is necessary for the Union to perform its functions and/or activities.

The Union collects, holds, uses and discloses your personal information for reasons including but not limited to:

- assisting you with industrial relations and employment queries;
- informing you about industrial, social and political campaigns;
- informing you about your rights at work;
- informing you about changes to legislation;
- referring you to a legal practitioner, accountant, translator or other professional;
- improving our service delivery;
- completing campaign petitions
- managing our relationship with you;
- conducting surveys and research;
- providing educational services and professional development;
- conducting Union elections; or
- other matters as required under legislation.

How do we collect Personal Information?

We will collect personal information directly from you via phone, Internet, hard copy form, email, social media, or in person unless:

- you have consented to the Union's collection of your personal information from third parties - for example, from the ACTU, or your representatives; or
- when we are legally required to do so; or
- it is unreasonable or impractical to collect it from you directly.

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.

What do we do with unsolicited information?

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 the information is not contained in a Commonwealth record, we will, if it is lawful and reasonable to do so, destroy or de-identify the information.

How does the Union hold personal information?

Wherever reasonably practicable, the Union holds electronic personal information on data servers that are owned and controlled by the Union in Australia. The data servers are password protected and login secured. However, by providing personal information to the Union you consent to your information being stored and processed on a data server or data servers (e.g. cloud services) owned by a third party or third parties that may be located outside of Australia. The Union will take reasonable steps to ensure that any third party providers comply with the APPs. If personal information is only routed through servers located outside of Australia – this is not regarded as a disclosure.

Wherever reasonably practicable, the Union holds physical personal information in access controlled premises.

When the Union no longer requires your personal information for a specific purpose and we are not required to keep it to comply with any laws, we will take such steps as are reasonable in the circumstances to destroy your personal information or to ensure that the information is de-identified.

Can I access and/or seek correction to personal information held by the Union?

You have the right to request access to your personal information and request that it be updated or corrected. In most cases you can gain access to your personal information that the Union holds. To request access to, correction of, or updating of any personal information held about you, please write to the Privacy Officer at the following address:

Privacy Officer
AMWU
PO Box 160
Granville NSW 2142

Or email: Privacy@amwu.org.au

General enquiries can be made via telephone by calling 1300 732 698:

The Union requires that you provide proof of identity in order to seek access to your personal information. The Union may refuse to provide access if permitted to do so by law or under the APPs. The Union will seek to provide you with access to your personal information within 30 days of receipt of a valid request.

Please ensure that your personal information details are up to date. The Union may also take steps to update your personal information by reference to publicly available sources such as telephone directories or electoral rolls, or may endeavour to call or email you to ensure your information is accurate, up to date, complete and relevant.

The AMWU Membership Department can be contacted at the following address:
amwu@amwu.org.au

What kinds of information does the Union website collect?

The Union 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 place 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.

You can adjust your Internet browser to disable cookies or to warn you when cookies are being used. However, if you disable cookies, you may not be able to access certain areas of the Website or take advantage of the improved web site experience that cookies offer.

What about the links to external sites?

Our websites may contain links to other websites and social media pages including Facebook and Twitter. We are not responsible for the privacy policies of the entities responsible for those websites and we recommend that you review the privacy policies applicable to any other websites you visit.

Do I have to give my name or other personal details when dealing with the union?

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 make comment 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.

Using your information for direct marketing

We will deem provision of personal information as 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, by unsubscribing, opting out or getting in touch with the Union.

Can I Unsubscribe or opt out of Direct Marketing?

Yes, If you no longer wish to receive direct marketing or other communications, you may request at any time to cancel your consent to such communications as follows:

- If subscribing to an email newsletter you may "unsubscribe" at any time from the newsletter mailing list, by clicking on the “unsubscribe” button at the bottom of the newsletter;
- The Union may, from time to time, send you text messages about issues of importance such as events or campaigns. You may “opt out” by texting STOP in reply to a text message from the Union; or
- You may contact us at any time by mail or email directed to our Privacy Officer.

To whom might we disclose your personal information?

The Union may disclose your personal information, in connection with or to further the purposes outlined above, to:

- the ACTU;
- other Australian trade unions;
- affiliated trades halls or labour councils;
- AMWU Delegates and AMWU Occupational Health & Safety Delegates;
- political parties;

- government bodies or agencies (including the Fair Work Commission, the Fair Work Ombudsman, the Australian Tax Office, an anti-discrimination body, a work/occupational health and safety regulator);
- organisations to whom we outsource functions (including information technology providers, print service providers, mail houses, debt collection agencies, insurance companies, call centres), market research;
- other global Unions e.g. IndustriALL, International Labour Organization;
- otherwise as you have consented; and/or
- otherwise as required by law.

The Union does not sell or licence your personal information to third parties. We take reasonable steps to ensure that each organisation that we disclose your personal information to is committed to protecting your privacy and complies with the Australian Privacy Principles, or is subject to a law or scheme that is at least substantially similar to the way in which the Australian Privacy Principles protect information.

By providing your personal information to the Union, you consent to us transferring your personal information to such other organisations.

How do we safeguard your information?

The AMWU will take all reasonable steps to ensure that the personal information it collects and stores is accurate, complete and current.

Personal information is kept in secured locations on 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. An electronic backup of information is maintained in a secure offsite facility and is only accessed by authorised personnel.

The AMWU may determine that the personal information obtained may be destroyed in accordance with our Disposal Schedule.

Notifiable 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 and the Australian Information Commissioner must be notified of an Eligible Data Breach.

Although *serious harm* is not defined by the Privacy Act, in the context of a data breach, *serious harm* to an individual may include serious physical harm, psychological harm, emotional harm, financial harm or reputational harm.

Examples of *serious harm* to an individual may include identity theft, significant financial loss by the individual, threats to an individual's safety, loss of business or employment opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalisation.

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 is 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.

Some examples of possible eligible data breaches include:

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;
5. A file containing details of a member(s) industrial matter is lost, stolen, or misplaced; or
6. An employee browses sensitive member information without any legitimate purpose.

It is of upmost importance and consistent with union values, that members personal information remains confidential. Our members have entrusted us to safeguard their information and a misuse of this may lead to reputational damage, loss of trust and personal damage to our members.

If an AMWU staff suspects a data breach may have occurred, they have an obligation to immediately report the breach to the National Secretary or Branch Secretary who will determine the next steps in line with the Data Breach Procedure.

Do we use Government Identifiers?

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

What about my privacy as a Job Applicant?

Where you provide information to the Union 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 Union. Where you provide the details of referees, you confirm that you have informed the referees that you are providing their contact information to the Union and they have consented to the Union contacting them and discussing the personal information you have provided in relation to the job application.

Can I make a complaint about a privacy breach?

Yes, to make a complaint about an alleged breach of the APPs please write to or email the Privacy Officer at one of the following addresses:

Privacy Officer
AMWU
PO Box 160
Granville NSW 2142

Or email: Privacy@amwu.org.au

All complaints must be in writing. Please provide all details about your complaint as well as any supporting documentation to the Privacy Officer. If you provided a pseudonym or dealt with the Union anonymously, it may be difficult to investigate such a complaint.

If you are dissatisfied with our response, you may refer the matter to the Australian Information (Privacy) Commissioner (see www.oaic.gov.au).

How will our Union deal with complaints?

The Union will seek to deal with alleged breach of the APPs by treating privacy complaints seriously, dealing with complaints promptly and confidentially and undertaking an investigation of complaints by the Privacy Officer.

The outcome of an investigation will be provided to the complainant where the complainant has provided proof of identity. The Union will seek to respond within 30 days of receipt of a valid complaint.

Variations to the Policy

This Policy may be varied from time to time and an updated version will be posted on the Union's websites. Please check our websites regularly to ensure that you have the most recent version of this Policy.

Version Control

Version Number	Approval Date & Meeting	Amendments
0-1	December 2001 – National Council	• Adopted Privacy Statement
0-2	March 2014 – National Council	• Detailed policy
0-3	December 2017 – National Council	• Minor amendments – who we disclose information to • Minor amendments - what information do we collect
0-4	March 2020 – National Council	• New heading – how we safeguard information • New heading – Notifiable Data Breaches • New process – Data Breach Procedure

Appendix A – Data Breach Procedure

The AMWU'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 the other information.

The AMWU and our external IT Support Provider will consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the AMWU 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 practical 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 that 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 the AMWU 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, the AMWU and external IT Support Provider will consider whether remedial action is possible.

If an assessment is required, the AMWU and our external IT Support Provider will follow a four-stage process as follows:

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

AMWU and our external IT Support Provider will conduct this assessment expeditiously and, where possible, within 30 days. If it cannot be completed within 30 days, we will include in the documentation why this is the case.

Where possible, the AMWU and our external IT Support Provider 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 or 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, the AMWU will prepare a statement for the Privacy Commissioner (a form is available of the Commissioner's website) that contains:

1. A description of the breach;
2. The kind(s) of information concerned; and
3. Recommended steps for individuals.

The AMWU will notify affected individuals and inform them of the contents of 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 practical:

- **Option 3:** Publish the statement on the AMWU website and publicise it.

When a breach requiring notification has occurred, the AMWU 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 plain is implemented;
- Updating the security / response plan;
- Considering changes to policies and procedures;
- Revising / providing staff training; and/or
- Engaging with our external IT personnel

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

- Police or law enforcement;
- Various professional bodies;
- APRA or the ATO;
- The Australian Cyber Security Centre; and or
- The AMWU financial service provider