



AUSTRALIAN
WAR MEMORIAL

Privacy Management Policy

Contents

Privacy Management Policy	5
OVERVIEW	5
1. Definitions	7
2. Personal information Collection (APP 1-5)	9
2.1 Personal Information collection	9
2.2 Sensitive Information collection	9
2.3 Collection of information from third parties	9
2.4 Notification of data collection	10
2.5 Unsolicited Personal Information	10
2.6 Anonymity and pseudonymity	11
3. Use and Disclosure (APP 6-9)	11
3.1 Use and disclosure of Personal Information	11
3.2 Direct Marketing	11
3.3 Cross-Border Disclosure	12
4. Accuracy of information (APP 10)	12
5. Security of Personal Information (APP 11)	12
5.1 Storage	12
5.2 Destruction	13
5.3 Notifiable Data Breach Plan	13
6. Access to Personal Information (APP 12-13)	13
6.1 Access to Personal Information	13
6.2 Correction of Personal Information	13
6.3 How to request access to or correction of Personal Information	14
6.4 How the Memorial will respond to a request to access or correct Personal Information	14
7. Register of Personal information holdings	15
8. Risk Management	15
8.1 Business Risk Register	15
8.2 Privacy Impact Assessments	15
9. Privacy Officers	15
9.1 Privacy Champion	15
9.2 Privacy Officer	15
9.3 Section Privacy Officer	15

9.4 Data Breach Response Officer	15
10. Privacy Training	16
11. Complaints about the memorial's privacy processes	16
11.1 Complaints	16
11.2 How the Memorial will respond to complaints about the handling of Personal Information	16
11.3 How to make a privacy complaint to the Office of the Australian Information Commissioner	16
12. Privacy Policy Updates	17
12.1 Update Schedule	17
12.2 Last review	17
13. Obtaining copies of this policy	17
13.1 Access	17
13.2 Alternative formats	17
13.3 Cost	17

PRIVACY MANAGEMENT POLICY

The Australian War Memorial (Memorial) takes the matter of information privacy seriously. It endeavours at all times to protect and handle personal information in a manner consistent with its obligations under the *Privacy Act 1988* (Privacy Act), the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, the Australian Privacy Principles (APPs) and the APP Code for Australian Government Agencies.

This policy has been developed and is maintained in accordance with the Australian War Memorial's Director's Instruction *9.02 Handling of Personal Information*.

OVERVIEW

The Memorial's purpose is to commemorate the sacrifice of those Australians who have died in war. Its mission is to assist Australians to remember, interpret and understand the Australian experience of war and its enduring impact on Australian society.

The Memorial deals with personal information in relation to its main functions as a memorial, museum and an archive and the activities that support these functions. Such activities include:

- Commemoration, ceremony or events
- Collections development and management
- Exhibitions development and management
- School education programs
- Fundraising, including retail operations
- Marketing
- Sponsorship and supporters programs
- Volunteer programs
- Personnel recruitment and contract management
- Communications including personal and corporate correspondence
- Social media and online activity

These and other activities often require the Memorial to collect contact information and personal details of individuals wishing to be involved in or have access to the Memorial's collections and programs.

All such activities are carried out by the Memorial in accordance with the powers and limitations of the *Australian War Memorial Act 1980*.

The Memorial carefully balances the need for information from those wishing to access its archives, programs and services with the amount and type of information it collects and the manner in which it stores, uses and shares this information.

The Memorial is also mindful of privacy issues when providing access to personal recollections, accounts and material held in the National Collection. These records may also

be subject to government regulations in relation to classified information and public access to records may also be withheld on these grounds.

This Privacy Management Policy outlines how we will comply with the Australian Privacy Principles (APPs) and the APP Code for Australian Government Agencies.

This Privacy Management Policy outlines how we will handle requests for access to or correction of personal information and complaints about our handling of privacy related matters.

1. DEFINITIONS

The key concepts and definitions used in this plan are contained in the Privacy Act and are outlined below:

Australian Privacy Principles (APP) are contained in the Privacy Act.

Consent means express consent or implied consent

Health information means:

- A) information or an opinion about:
 - i) the health or a disability (at any time) of an individual; or
 - ii) an individual's expressed wishes about the future provision of health services to him or her; or
 - iii) a health service provided, or to be provided, to an individual; that is also personal information; or
- B) other Personal Information collected to provide, or in providing, a health service; or
- C) other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- D) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Personal information is defined in the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.'

The types of Personal Information that the Memorial collects and holds will depend on the circumstance and relationship between the individual and the Memorial.

Personal information that is commonly collected by the Memorial includes:

- Name
- Address (residential, postal and email)
- Phone number
- Date of birth
- Gender
- Country of Birth
- Driver's Licence
- Banking and superannuation details
- Tax File Number
- Health information

- Emergency contact details
- Photographs or video recordings (including ID cards, CCTV footage and event photography/videography)
- Criminal history
- IT access logs
- Records of donations and related family histories
- Retail or other transactional records
- Security Clearance status

Privacy Statement means a notification, in the format specified under paragraph 2.2, that is required to be provided to an individual at or before the time (or, if that is not practicable, as soon as practicable after) the Memorial collects Personal Information.

Sensitive information is defined in the Privacy Act as:

- A) Information or an opinion about an individual's:
 - i) racial or ethnic origin; or
 - ii) political opinions; or
 - iii) membership of a political association; or
 - iv) religious beliefs or affiliations; or
 - v) philosophical beliefs; or
 - vi) membership of a professional or trade association; or
 - vii) membership of a trade union; or
 - viii) sexual orientation or practices; or
 - ix) criminal record that is also Personal Information;
- B) Health information about an individual;
- C) Genetic information about an individual that is not otherwise health information; or
- D) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- E) Biometric templates.

Memorial Personnel means all employees, appointed office holders (Council), consultants, contractors and volunteers of the Memorial.

2. PERSONAL INFORMATION COLLECTION (APP 1-5)

2.1 Personal Information collection

Personal information must only be collected by lawful and fair means and only when it is reasonably necessary or directly related to the Memorial's activities.

Collection must not be unreasonably intrusive nor should it be collected on the basis that it may be useful in future.

Example: When collecting information relating to booking a seat at a commemorative event only an email address needs to be collected to alert attendees to critical event changes. Information not necessary for this specific purpose, such as a home address or landline telephone number, should not be collected. If the Memorial is seeking additional information, such as postcode of residence, for demographic or research purposes it should be clearly labelled as such and the process should make provision of that data as 'opt-in' only.

2.2 Sensitive Information collection

Memorial Personnel must generally only collect Sensitive Information with the individual's consent and when the information is reasonably necessary for one or more of the Memorial's functions or activities.

Example: Racial or ethnic information may only be collected from job applicants in relation to Identified or Special Measures employment opportunities and only with the express consent of applicants.

There are limited circumstances where consent is not required as outlined in the APP, the exemptions most likely to apply to the Memorial relate to security matters and include:

- Instances where it is unreasonable or impracticable to obtain consent and the Memorial has a reasonable belief that the information is needed to lessen or prevent a serious threat to the life, health or safety of an individual or the public; or
- the Memorial has a reasonable belief that the information is needed in order to take action on suspected unlawful activity or misconduct of a serious nature

Example: Memorial Personnel attending a medical emergency may collect Sensitive Information regarding a person's health from a third party or personal effects in order to perform first aid.

2.3 Collection of information from third parties

Where possible, Memorial Personnel must collect Personal Information only from the individual concerned. If Personal Information about an individual is collected from another source, Memorial Personnel must take reasonable steps to ensure that the individual is or has been made aware the Memorial has collected the information and provided with an approved Privacy Statement.

Example: Bequest or donor information is sent to individuals on a mailing list acquired from a third party - the Memorial should ensure that communication with persons on this list includes how the Memorial obtained their personal information and an approved Privacy Statement.

2.4 Notification of data collection

Where Personal Information is collected or solicited from forms or websites, Memorial personnel should ensure that an approved Privacy Statement is included on the web page or form.

Where Personal Information is specifically sought through personal contact (e.g. on-site surveys; phone; onsite Research Centre enquiries) Memorial Personnel must inform the individual of the data being collected and availability of the Privacy Policy on the Memorial's website.

This may be achieved through a verbal Privacy Statement or for common on-site activities through the use of approved Privacy Statement signage.

Example: Signage with an approved Privacy Statement should be clearly visible within the Research Centre to inform visitors that personal information may be collected in order to provide appropriate access to materials held in the National Collection.

Privacy Statements should be tailored depending on the level of information collected and the purpose for which it is used. Privacy Statements can be approved by Section or Branch Heads.

Approved Privacy Statements must include at a minimum:

- A contact phone number or email for requests for information or complaints
- Information on where the Memorial's Privacy Policy can be found
- whether the information will be disclosed to a third party
- Any significant consequences if information is not provided

Example: A Privacy Statement included in relation to volunteering or staff recruitment should note that 'If you do not provide the required information your application may not be processed or assessed.'

2.5 Unsolicited Personal Information

Unsolicited Personal Information is information that the Memorial receives but did not actively seek to collect.

Unsolicited Personal Information that is not reasonably necessary or directly related to the Memorial's functions or activities must be destroyed or de-identified, unless it is necessary to preserve the document in order to comply with recordkeeping obligations. If retained it should be treated in accordance with the principles in this plan.

Example: An unsolicited CV is sent to the Memorial and retained for consideration of future job opportunities, the sender should be informed the Memorial has retained their Personal Information and provided with a suitable Privacy Statement.

2.6 Anonymity and pseudonymity

Wherever practicable the Memorial will provide the opportunity for people to deal with us anonymously or pseudonymously.

Example: Surveys should only include fields for name, email address or phone number if the Memorial intends to follow up with the individual completing the survey.

3. USE AND DISCLOSURE (APP 6-9)

3.1 Use and disclosure of Personal Information

Personal information is valuable, and its loss or unintended disclosure can have significant consequences for the individual and for the Memorial.

The Memorial will generally only use or disclose Personal Information for the purpose of conducting activities in accordance with the *Australian War Memorial Act 1980* or where an individual would reasonably expect the Memorial to use or disclose the information for another purpose.

Example: The Memorial may use an email address provided as part of a research enquiry to contact the correspondent for the purposes of conducting that research. The Memorial may not use that information for general mailing list activities unless the correspondent has specifically 'opted-in' to receive such email.

The Memorial may also use or disclose Personal Information for another purpose in special circumstances as allowed for within the Privacy Act, such as with the individual's consent or for health and safety or law enforcement reasons.

Example: The Memorial receives a direction from the Freedom of Information Ombudsman to release Personal Information in relation to an FOI request.

The Memorial may also hold classified or restricted Personal Information, this information is treated in accordance with both the APP and other legal requirements.

There is a general right of access to some archival records held by the Memorial in relation to the Australian Defence Force once they are in 'open access'. The Memorial's Research Centre manages access to these records in accordance with the relevant Director's Instruction.

3.2 Direct Marketing

Direct marketing, distributing information about the Memorial directly to an individual using Personal Information, is only permissible for activities in accordance with the *Australian War Memorial Act 1980* or where the Memorial has obtained express consent to use Personal Information for this purpose.

All direct marketing activities must include an 'opt-out' method and the Memorial must honour requests to opt out of direct marketing within 7 working days.

3.3 Cross-Border Disclosure

The Memorial will only transfer information outside Australia within the limited circumstances provided for within the Privacy Act.

Unless express consent has been given for cross-border transfer the Memorial must only do so after conducting a Privacy Impact Assessment (PIA) and only when it is assured that the cross-border party is willing and able to manage the information in accordance with the APPs.

Example: The Memorial must conduct a PIA prior to transferring Personal Information to a cloud service including assessing the location of the server(s) the information will be held on and assuring itself that the company and nation of holding will do so in accordance with the APPs.

4. ACCURACY OF INFORMATION (APP 10)

The Memorial will make all reasonable efforts to ensure the Personal Information it holds is accurate and up to date.

Example: The Memorial sends a letter and the recipient responds noting a change in address, the Memorial must make every effort to update this address in all relevant databases.

5. SECURITY OF PERSONAL INFORMATION (APP 11)

5.1 Storage

Personal information must be stored securely to prevent loss or misuse. The Memorial makes all practicable efforts to ensure that Personal Information is held securely. Access to this information is only available to employees to enable them to conduct the required tasks of their role.

The Memorial retains information in accordance with its legal record keeping obligations, internal policies including those relating to management of the National Collection and the APPs.

Personal information in electronic format must be stored and managed securely in accordance with the Director's Instructions (Administrative).

Financial information, including credit card and personal banking information, must be handled in accordance with the Director's Instructions (Financial) and related procedures.

Hardcopy records containing Sensitive Information should be stored in locked furniture when not in use. Access should only be available to authorised personnel and should not be used in places visible to members of the public.

5.2 Destruction

Personal Information no longer needed for the purpose it was collected, and not otherwise required to retain the information under any law, regulation or code must be destroyed in a secure manner or de-identified.

5.3 Notifiable Data Breach Plan

The Memorial maintains and regularly reviews a Notifiable Data Breach Plan (NDBP) in order to respond to any loss or breach of personal information held by the Memorial.

The NDBP sets out procedures and lines of authority in the event that the Memorial experiences a data breach (or suspects that a data breach has occurred).

This Plan is intended to enable the Memorial to contain, assess and respond to data breaches in a timely fashion and to mitigate potential harm to affected individuals.

6. ACCESS TO PERSONAL INFORMATION (APP 12-13)

6.1 Access to Personal Information

Individuals (other than Memorial Personnel) who request access to Personal Information about themselves held by the Memorial must submit their request through the Memorial's Freedom of Information officer.

The Freedom of Information officer will process requests in accordance with relevant Director's Instructions (Administrative).

Memorial Personnel requesting access to their employment related Personal Information are entitled to do so without filing an FOI request, requests are managed by the Head, Human Resources in accordance with the relevant Director's Instructions (Administrative).

The Memorial may, in accordance with general FOI principles, limit access to documentation requested by both Memorial Personnel and other individuals including when:

- Access would unreasonably impact another individual's privacy
- Documents are subject to confidentiality obligations (such as a written reference for employment), legal privilege or contain commercially or legally sensitive information
- Where requests are vexatious or frivolous

Memorial Personnel provided with limited access to their Personal Information may file a formal FOI request for release of same.

In accordance with the principles of *Use and disclosure of Personal Information* as outlined in this policy, the Memorial may grant access to Personal Information to third parties such as law enforcement agencies or an Ombudsman's office.

6.2 Correction of Personal Information

An individual can request Personal Information held by the Memorial is corrected, including amending, deleting or adding to a record, to ensure the information is accurate, up to date, complete and not misleading.

The Memorial will amend records where practicable and reasonable within 30 days of a request and will notify the individual the requested change has been made.

The Memorial may request proof of identity or of accuracy of a requested change.

Example: A member of staff requests the Memorial updates their personnel record to reflect the award of an academic or other qualification, the Memorial may request proof of conferment before doing so.

The Memorial may deny such requests where it is contrary to the public interest or its record keeping or collections management obligations to do so. The Memorial will provide a written response outlining the reason why the request was denied in such circumstances and information on how the correspondent can complain or have this decision reviewed.

Example: An individual requests the Memorial alter details held in records held by the National Collection, the Memorial may refuse this request so as not to adversely impact the historical accuracy of a document.

The Memorial may make alterations to records directly or through notation.

You will not be charged for lodging a request to access or correct personal information.

6.3 How to request access to or correction of Personal Information

If you wish to access or correct personal information we hold about you, you may:

- Email: executive@awm.gov.au
- Write to:
Privacy Officer
Australian War Memorial
GPO Box 345
Canberra ACT 2601
AUSTRALIA
- Phone: the Memorial's switchboard on +61 (02) 6243 4211

6.4 How the Memorial will respond to a request to access or correct Personal Information

If you have provided contact details the Memorial will acknowledge your request within 5 business days.

If you have provided contact details the Memorial will provide you with a written response within 30 days after receiving your request, by:

- providing access to the documents;
- advising you of our decision to refuse access to or correction of documents; or
- advising you of any difficulties we have encountered in completing your request, in which case we will provide you with an updated timeframe for finalising your request.

If your request requires a significant number of documents or requires consultation with other parties, we may ask you to make a request under the *Freedom of Information Act 1982*, in order to provide a clear structure for our response to your request.

7. REGISTER OF PERSONAL INFORMATION HOLDINGS

The Memorial publishes a register of Personal Information it holds online:

<https://www.awm.gov.au/about/organisation/corporate/information-publication-scheme/pid>

The register is periodically reviewed and updated.

8. RISK MANAGEMENT

8.1 Business Risk Register

The Memorial takes privacy matters seriously and management of its privacy obligations is listed on its Business Risk Register and managed in accordance with the relevant Director's Instructions (Administrative).

8.2 Privacy Impact Assessments

The Memorial will undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information.

The privacy risks of Memorial projects will be assessed as part of the standard Risk Assessment process of standing up a new project.

The Memorial keeps a register of all PIAs conducted and publishes a summary of this information on its website.

9. PRIVACY OFFICERS

9.1 Privacy Champion

The Memorial designates the Assistant Director, Corporate Services as the 'Privacy Champion' for the purposes of the Australian Government Agencies Privacy Code.

9.2 Privacy Officer

The Memorial designates the Executive Officer, Corporate Services as the 'Privacy Officer' for the purposes of the Australian Government Agencies Privacy Code.

9.3 Section Privacy Officers

Within each functional area of the Memorial (Section) a Privacy Officer is nominated to provide advice or assessment on privacy matters as they apply to each Section.

9.4 Data Breach Response Officer

Under the Memorial's Notifiable Data Breach Response plan the IT Business Team Leader is appointed as the Data Breach Response Officer (DBRO). The DBRO is the initial point of contact for suspected or known breaches and provides advice and assistance to the CIO and Privacy Champion in reviewing reported breaches.

10. PRIVACY TRAINING

The Memorial provides information on privacy obligations to all staff as part of the staff induction process. Memorial staff who regularly deal with personal information are also required to undertake annual refresher training in relation to privacy matters.

The Memorial provides staff with access to the APS Privacy Awareness training module through its eLearning system.

Memorial staff designated as either a Privacy Champion or Privacy Officer receive additional support such as access to the OAIC Privacy Officer Toolkit or training opportunities to properly equip them for their role.

11. COMPLAINTS ABOUT THE MEMORIAL'S PRIVACY PROCESSES

11. Complaints

Complaints about the collection, sharing, handling or correction of your personal information by the Memorial can be made by the following means:

- Email: executive@awm.gov.au
- Write to:
Privacy Officer
Australian War Memorial
GPO Box 345
Canberra ACT 2601
AUSTRALIA
- Phone: the Memorial's switchboard on +61 (02) 6243 4211

11.2 How the Memorial will respond to complaints about the handling of Personal Information

If you have provided contact details the Memorial will acknowledge that we have received your complaint within 5 business days.

If you have provided contact details the Memorial will respond to your privacy complaint within 30 calendar days of receipt of the complaint.

The Memorial is committed to transparent, quick and fair resolution of customer complaints and will ensure any privacy complaint is taken seriously.

11.3 How to make a privacy complaint to the Office of the Australian Information Commissioner

If you are dissatisfied with the way the Memorial has handled any aspect of your personal information or a request to access or correct same you may contact the Office of the Australian Information Commissioner (OAIC):

- Email: privacy@privacy.gov.au
- Write to:
Office of the Australian Information Commissioner

GPO Box 5218
Sydney NSW 2001

- Use the online complaint form at the OAIC website:
<https://www.oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint>

Please note that the OAIC is unable to receive complaints over the phone.

12. PRIVACY POLICY UPDATES

12.1 Update Schedule

This policy will be reviewed annually at a minimum, or more frequently as required, including when the OAIC guidance material is revised or legislative amendments are made to the Privacy Act.

12.2 Last review

This policy was last reviewed: 5 September 2018

13. OBTAINING COPIES OF THIS POLICY

13.1 Access

This policy and associated documents are published in PDF and web page on our website:
www.awm.gov.au.

13.2 Alternative formats

If you wish to access this policy in an alternative format or hard copy, please [contact the Memorial](#).

13.3 Cost

A single copy of this policy and associated documentation will be provided at no cost upon request.