Privacy Policy

1. Purpose

The purpose of this policy is to set out how ARPC collects, uses, discloses, and stores personal information, and how individuals may access and correct the personal information that ARPC holds about them.

This Policy is mandatory for all employees, Board members, contractors and consultants engaged by ARPC.

Failure to comply with this Policy and related procedures may result in disciplinary action being taken in accordance with the ARPC disciplinary procedure.

2. Policy Statement

ARPC is a Corporate Commonwealth entity within the Treasury Portfolio and provides insurance cover for eligible terrorism losses and cyclone and cyclone related flood damage to houses, small businesses, and strata.

Treasury is a separate agency under the Privacy Act and may also hold personal information in relation to ARPC employees and Members, as part of the provision of Treasury financial services to ARPC. The Treasury's Privacy Policy is available on its website and details how it will manage any personal information that it holds.

ARPC is committed to complying with its obligations under the Privacy Act. ARPC will manage your personal information in accordance with the Privacy Act and Australian Privacy Principles (APPs) which regulate how ARPC may collect, use, disclose and store personal information, and how individuals may access and correct the personal information that is held about them.

3. Personal information handling practices

3.1. The kinds of information we collect and hold

The kinds of personal information we collect, and hold will depend on the function or activity being undertaken. Examples of personal information ARPC collects and holds include:

- documents relating to employment of staff and Board Members (for example names, signatures, dates of birth, contact information, government related identifiers such as Tax File Numbers, financial information, photos, health information, emergency contacts, identification, information relevant to obtaining and maintaining a security clearance);
- documents relating to recruitment and selection processes (for example qualifications, information about an individual's background and personal circumstances, work history, referees' reports, social media posts and police checks);
- documents relating to appointments to Commonwealth Boards (for example register of interests, qualifications, and work history);
- documents relating to claims from insurers (for example details of contact person and claims assessor's reports);
- distributions, mailing lists and contact lists (for example telephone numbers, business address and email addresses);
- enquiries to ARPC and ministerial correspondence (for example names and contact details);

- details of visitors to ARPC premises (for example names and organisation, contact details, date, and time of visit);
- financial and other information about tenderers, suppliers, contractors, consultants, customers, and research partners (for example names, contact information and banking details); and
- information provided in the course of making submissions or requests under the *Freedom of Information Act 1982* (FOI Act).

3.2. Sensitive information

On occasion, ARPC may collect or hold sensitive information, such as personnel and board member records. The Privacy Act defines sensitive information as:

- information or opinion about an individual's racial or ethnic origin, political opinion, membership of political or professional or trade associations or unions, religious and philosophical beliefs, sexual orientation or practices or criminal record, provided the information or opinion otherwise meets the definition of personal information,
- Health information about an individual,
- Genetic information about an individual,
- Biometric information that is to be used for the purpose of automated biometric verification or identification, and biometric templates.

3.3. How we collect personal information

ARPC generally collects personal information from you directly or through your authorised representatives. ARPC will only collect your personal information where it is reasonably necessary for, or directly related to, its functions or activities.

ARPC may sometimes collect your personal information from a third party or from a publicly available source, but only if:

- you express or imply consent (unless it is unreasonable or impracticable to collect the personal information from you); or
- ARPC is required or authorised to do so by or under an Australian law or court or tribunal order.

ARPC may collect your sensitive personal information with your express or imply consent when it is necessary for, or directly related to, the performance of our functions or activities, or the collection is required or authorised by law.

The Privacy Act also allows ARPC to collect your sensitive information in certain other exceptional circumstances, including where a permitted general situation exists (for example to lessen or prevent a serious threat to life, health, or safety).

From time to time, personal information is provided to ARPC without it being requested (for example, where a letter is sent to ARPC, or an enquiry is made). When such information is received ARPC will handle your information in accordance with its obligations under the Privacy Act.

3.4. Use and disclosure

ARPC will ordinarily only use and disclose your personal information for the primary purpose for which it was collected. For example, to respond to an enquiry during a Declared Terrorist Incident, Declared Cyclone Event, or to process an insurance claim.

ARPC may also use or disclose your personal information for a purpose related to, or directly related to, the purpose of collection where you would reasonably expect that your information would be used or disclosed for this other purpose.

We may use or disclose your personal information for another purpose permitted by the Privacy Act and the APPs, including where:

- you express or imply consent
- ARPC is required or authorised by or under the *Terrorism and Cyclone Insurance Act 2003* (TCI Act)
- a permitted general situation exists as defined in the Privacy Act (for example, to take action in relation to suspected unlawful activity or serious misconduct)
- a permitted health situation exists as defined in the Privacy Act
- ARPC reasonably believes that the use or disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

ARPC may disclose information about your attendance at its premises for the purpose of contact tracing.

ARPC does not generally disclose personal information to overseas recipients. If it is necessary for ARPC to disclosure your personal information outside Australia, the obligations under APP 8 (Cross-border disclosure of personal information) will be met.

3.5. Privacy notices

ARPC will undertake all reasonable steps to notify you at the time it collects your information, or shortly after, if the information is likely to be passed on to another body and, if relevant, provide details of the bodies to which the information is likely to be given.

3.6. Data security

ARPC holds personal information on paper files (minimal), electronic files, and databases. ARPC uses a range of physical and electronic security measures to protect your personal information from misuse and loss and from unauthorised access, modification, or disclosure. For example, ARPC restricts physical access to its offices, employs security containers, firewalls, secure databases, secure online payment systems, computer user identifiers and passwords.

3.7. Data accuracy

ARPC takes all reasonable steps to validate that the personal information collected is accurate, up-to-date, complete, relevant, and not misleading.

3.8. ARPC website

No attempt will be made to identify individual users of the ARPC website or their browsing activities except, in the unlikely event of an investigation, where a law enforcement agency may exercise its authority to inspect the Internet Service Provider's log files.

3.9. LinkedIn

We use LinkedIn to engage with the public and our staff and we may collect, use, and disclose personal information through that site. LinkedIn has its own privacy policy concerning how it handles personal information accessible on its website.

3.10. Privacy Management Plan

ARPC has a Privacy Management Plan, as per the Privacy (Australian Government Agencies Governance APP) Code 2017 (Privacy Code), that supports the Privacy Policy. The Plan outlines how ARPC:

- Manages personal information in accordance with APP 1.2;
- Delivers training, education and awareness to staff addressing ARPCs privacy obligations;
- Identifies and responds to privacy breaches; and
- Measures and documents its performance against the plan.

3.11. Privacy Impact Assessment (PIA)

Where ARPC undertakes a project that may involve the handling of personal information in any new or changed ways, and which are likely to have a significant impact on the privacy of individuals, a PIA will be conducted pursuant to the obligations set out by the Privacy Code. ARPC maintains a Privacy Impact Register for all high privacy risk projects. The PIA Register is published on ARPC's Website.

3.12. Dealing with ARPC anonymously or pseudonymously

Where it is practicable, you may choose to remain anonymous or adopt a pseudonym when dealing with us. For example, if you make an enquiry or complaint. However, in certain situations it will be necessary for us to collect your name and other personal details.

4. Roles and Responsibilities

Role	Key Responsibilities
Board	Approval and oversight of the Privacy Policy.
Audit Compliance Committee (ACC)	Reviewing and recommending the Privacy Policy to the Board and monitoring its implementation.
Chief Executive Officer (CEO)	• Responsible for establishing and maintaining appropriate systems of internal control • Approval of procedures and non-material changes to existing policies. • Principal Executive for Privacy Act purposes and compliance with the Privacy Code 2017 including designation of a Privacy Officer and Privacy Champion.
Chief Operations Officer (COO)	Responsible for updating this Policy as required, and for taking reasonable steps to make it freely available. This Policy will be reviewed at least every three years, and will be updated whenever there are significant changes in: • Legislation; • Other ministerial or departmental guidelines; • Operations; • Key stakeholders; or • Systems.
Privacy Officer (CRO)	ARPC's designated Privacy Officer, the Chief Risk Officer (CRO), is responsible for: • Providing privacy advice internally, including assessing projects that may involve the handling of personal information in any new or changed ways, and which may have a significant impact on the privacy of individuals, to inform a decision on whether a PIA is required; • Liaising with the OAIC; • Coordinating the handling of internal and external privacy enquiries, complaints, and requests for access to, and

Role	Key Responsibilities
	correction of personal information; • Maintain a register of PIAs; and • Measuring and documenting ARPC's performance against the Privacy Management Plan.
Privacy Champion (COO)	ARPC's designated Privacy Champion, the Chief Operations Officer (COO), is responsible for: • Providing strategic direction to the management of personal information; • Promoting a culture of privacy that values and protects information; • Reporting to the CEO and ARPC Board on personal information data breaches, including any privacy issues arising from ARPC's handling of personal information; • Reviewing and/or approving the Privacy Management Plan; and • Documenting reviews of ARPC's progress against the Privacy Management Plan at least once each calendar year.
All staff	All staff must adhere to this Policy and the Australian Privacy Principles (APPs) and report any privacy breaches by any employee or contractor to the Privacy Officer and/or Privacy Champion as soon as they become aware of them.

5. Breach of Policy

5.1. Privacy breach

Any suspected privacy breach that is brought to the attention of ARPC will be investigated. We will treat any suspected privacy breach seriously and deal with it promptly.

5.2. Notifiable Data Breaches scheme

The Notifiable Data Breaches (NDB) scheme under Part 111C of the Privacy Act requires agencies to notify individuals and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individual whose personal information is involved in the breach. In general terms, 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.

If ARPC has reasonable grounds to believe that an eligible data breach has occurred, the Privacy Officer will promptly notify affected individuals and the OAIC through a statement about the eligible data breach.

6. Access to and correction of personal information

You have a right to request access to your personal information and to request correction of your personal information if it is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

If you wish to obtain access or seek correction of your personal information, please contact our Privacy Officer through one of the following means in the first instance:

Post Privacy Officer
Australian Reinsurance Pool Corporation
PO Box Q1432
Queen Victoria Building, NSW 1230

Email enquiries@arpc.gov.au
Telephone 02 8223 6771

Your request should identify the information you seek to access or correct and provide your contact details including an email address or mailing address.

Before providing access to or correcting your personal information, we may require you to verify your identity. There are no charges under the Privacy Act.

ARPC will respond to your request within 30 days of the request being made. If your request is refused, we will provide you with a written notice setting out the reasons for the refusal and information about how you can make a complaint. Where a correction is refused, you may also request an annotation.

Information about how to request information under the FOI Act is available here.

7. Privacy complaints

If you wish to make a privacy complaint, you should submit a written complaint to the contact details above. We will respond to your complaint within 30 days.

Where an investigation is conducted following a complaint, ARPC will advise the complainant of its outcome.

If you are not satisfied with our response, you may make a written complaint to the OAIC setting out why you consider the ARPC has interfered with your privacy. The OAIC will generally expect you to complain to ARPC first and will likely refer your complaint to us if you have not done so already. You may contact the OAIC by submitting a complaint online or via:

Post GPO Box 5288 Sydney NSW 2001
Email enquiries@oaic.gov.au
Phone 1300 363 992.

Policy Information Table

Accountable Officer	Chief Operating Officer
Approved By & Date	ARPC CEO (non-material amendments), 19/8/2024
Version Number	2.7
Commencement Date	19/8/2024
Relevant Legislation	Privacy Act 1988
Related Policies	ARPC Values ARPC Code of Conduct
Related Procedures	Information Security Procedure
Related Processes and forms	Privacy Management Plan
Key Terms & Definitions	Link to Glossary

Version control and history

Date	Version	Author	Summary of changes/circulated to/approved by
12 March 2014	0.1	Alison Kelly	New Policy
12 March 2014	0.1	Alison Kelly	Endorsed by Alison Kelly for publication (legislative requirement), email approval notification.
18 March 2014	0.2	Garry Boyd	Minor amendments following management review through Governance, Risk and Assurance meeting. Published.
7 May 2014	1.0	Wendy Cull	Approved version transitioned to template for publication.
31 March 2015	1.1	Wendy Cull	Minor amendments for title changes.
23 January 2018	2.0	Joshua Everson / Tracey Tai	Minor amendments and inclusion of reference to the Australian Govt Privacy Principle Code.
19 April 2018	2.1	Joshua Everson / Tracey Tai	- Addition of a breaches section including references to the Notifiable Data Breaches regime. - Amendments made to reflect organisational restructure of roles.
22 June 2018	2.2	Michaela Flanagan / Tracey Tai	Updated following AGS and Board review to incorporate comments.
29 June 2018	2.3	Michaela Flanagan / Tracey Tai	- Updated and finalised to meet Privacy Code obligations. - Approved by Board Members by circular resolution via email.
16 July 2018	2.4	Tracey Tai	Ratified by Board Members.
Aug 2021	2.5	Alanna O'Meara	- Policy reviewed and updated by AGS 31 March 2021 - Revised policy updated in new template. - Board approved 21 September 2021
29 July 2022	2.6	Alanna O'Meara	- Privacy Officer changed from Chief Financial Officer to Chief Risk and Governance Officer
30 July 2024	2.7	Alanna O'Meara	- Minor amendments to wording throughout document including roles and responsibilities table. - Privacy Officer changed from Chief Risk and Governance Officer to Chief Risk Officer

Appendix: Privacy Act Glossary

Key terms	Definition
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Government related identifier	Government related identifier (e.g., Medicare or tax file number) of an individual means an identifier of the individual that has been assigned by: (a) an agency; or (b) a State or Territory authority; or (c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or (d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.
Individual	Means a natural person.
Sensitive information	(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; or (b) health information about an individual; or (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.
Holds	An entity holds personal information if the entity has possession or control of a record that contains the personal information.
Use	An APP entity i.e., ARPC, uses information where it handles or undertakes an activity with the information, within the entity's effective control.
Disclose	Discloses personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.
Primary purpose	The purpose for which an APP entity i.e., ARPC, collects personal information is known as the 'primary purpose' of collection.