PRIVACY POLICY

AIMS-IC-03

Document Details

Implementation date:	8 September 2003	Authorised by:	Council
Edition No:	4	Responsible Officer:	Privacy Officer (General Counsel)
Date of Issue:	8 December 2020	Review date:	7 December 2023

TABLE OF CONTENTS

About this policy

The Privacy Act 1988 requires entities bound by the Australian Privacy Principles to have a privacy policy. This privacy policy outlines the personal information handling practices of the Australian Institute of Marine Science (AIMS). This policy applies to personal information we collect. It describes how we handle that personal information.

This policy is written in simple language. AIMS' specific legal obligations when collecting and handling your personal information are outlined in the *Privacy Act 1988* (Cth) and in particular in the Australian Privacy Principles found in that Act. This policy uses terminology that is consistent with the Act and the Principles. For example, the terms "personal information" and "sensitive information" have specific, defined meanings in the Act.

We will update this privacy policy when our information handling practices change. Updates will be published on our website (www.aims.gov.au).

Overview

We collect, hold, use and disclose personal information to carry out our functions or activities under the *Australian Institute of Marine Science Act 1972* (Cth).

These functions include:

- arranging and carrying out research and development in relation to marine science and marine technology, and the application and use of marine science and marine technology;
- encouraging and facilitating the application and use of the results of that research and development;
- co-operating with other institutions and persons in carrying out that research and development;
- providing other institutions or persons with facilities for carrying out research and development of that kind;
- collecting and disseminating information relating to marine science and marine technology, the application and use of marine science and marine technology and, in particular, to publish reports and other papers;
- producing, acquiring, providing and selling goods, and providing services, in connection with marine science and marine technology, and the application and use of marine science and marine technology;
- making available to other persons, on a commercial basis, our knowledge, expertise, equipment, facilities, resources and property; and
- doing anything incidental or conducive to the performance of any of those functions.

1. Collection

Our collection of your personal information

We try to collect only the information we need for the function or activity we are carrying out.

The main way we collect personal information about you is when you give it to us. We collect and hold a broad range of personal information about:

- our employees and people who apply for jobs at AIMS;
- our partners, collaborators, contractors, visitors, students and other stakeholders; and
- our research and operational activities.

We collect this information in a variety of ways, including in:

- online and paper-based forms;
- notes of meetings;
- electronic and hard-copy correspondence and documents;
- electronic systems;
- phone calls;
- photographs;
- audio or video recordings; and
- messages on social media.

Collecting sensitive information

Sometimes we may need to collect sensitive information about you, for example, to manage your employment at AIMS, your access to AIMS' sites or your involvement in our research activities. This might include information about your health, racial or ethnic origin, association memberships, or criminal history.

Indirect collection

In the course of managing and carrying out our functions and activities, we may collect personal information (including sensitive information such as health information) about you from third parties such as your nominated representatives or our partners, collaborators, contractors or other stakeholders.

We also collect personal information from publicly available sources.

Anonymity

Where possible, we will allow you to interact with us anonymously or using a pseudonym. For example, if you contact our Reception by phone or email with a general question about us or our activities we will not ask for your name unless we need it to adequately handle your question.

However, for most of our functions and activities we usually need at least your name and contact information and enough information about the particular matter to enable us to perform our functions and activities.

Collecting through our electronic systems

When you use our electronic systems and equipment (including our network, IT applications and AIMS-issued devices such computers and mobile phones), our IT and network protection systems collect and monitor usage and traffic, which may include your personal information.

For example, our intrusion detection system uses a process of complete raw packet capture of all data and sent and received by devices that are connected to our network. The purpose of this collection is to secure and protect our systems from cyber threats and is carried out in line with applicable laws and Commonwealth policies. We also apply strict controls on who at AIMS can access that data and the very limited circumstances in which that access can be given. Access by AIMS officers to the raw packet capture referred to above is only for the purpose of securing and protecting our systems from cyber threats.

Collecting through our website

For more information about the personal information collected by AIMS' website, see https://www.aims.gov.au/docs/privacy-policy.html.

Social media services

We use social media services such as Twitter, Facebook and LinkedIn to communicate with the public about our research and operations. When you communicate with us using these services we may collect your personal information, but we only use it to help us to communicate with you and the public. Usually, social networking services will also handle your personal information for their own purposes. These services have their own privacy policies. You can access the privacy policies for these services on their websites.

2. Disclosure

Our policy is to use and disclose the personal information we collect only for purposes directly related to our functions and activities (as outlined above) and only where it is necessary for, or directly related to, those purposes.

Some situations in which we may disclose information are detailed below.

Disclosure to service providers

We use some service providers to whom we disclose personal information. These include providers that host our website servers, manage our IT systems and manage our human resources information. To protect the personal information we disclose we generally:

- enter into a contract or MOU which requires the service provider to only use or disclose the information for the purposes of the contract or MOU; and
- include special privacy requirements in the contract or MOU, where necessary.

Disclosure of sensitive information

We only disclose your sensitive information for the purposes for which you gave it to us or for directly related purposes you would reasonably expect or if you agree, for example, to manage your involvement in our research activities.

Disclosure in an emergency

We may use or disclose your personal information (including some sensitive information such as health information) in an emergency situation if it is unreasonable or impracticable to obtain your consent to the use or disclosure and we reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety. For example, we may disclose your personal information to medical practitioners and others if you are injured while undertaking field work with us.

Disclosure of personal information overseas

Generally, we only disclose personal information overseas in limited circumstances. For example, we may disclose personal information overseas if an overseas referee is nominated to support a job application, you are involved in a secondment to or from an overseas post or we are applying for an international grant or working with a collaborator that is based overseas.

Web traffic information may be disclosed to others (for example, web traffic analysts) when you visit our websites. Those analysts may store that information across multiple countries.

When you communicate with us through a social network service such as Facebook, Twitter or LinkedIn, the social network provider and its partners may collect and hold your personal information overseas.

Disclosure under other laws

There may be circumstances in which we are required to disclose personal information to comply with other laws or regulations. For example, we may be required to disclose information under the *Freedom of Information Act 1982* (Cth), the *Public Governance, Performance and Accountability Act 2013* (Cth), the *Work Health and Safety Act 2011* (Cth) or the *Safety, Rehabilitation and Compensation Act 1988* (Cth).

3. Quality of personal information

To ensure that the personal information we collect is accurate, up-to-date and complete, we take steps that are appropriate to the type and quantity of information collected. For example, we:

- record information in a consistent format (to the extent that our systems allow);
- where necessary, confirm the accuracy of information we collect from a third party or a public source; and
- promptly add updated or new personal information to existing records (to the extent that our systems allow).

4. Storage and security of personal information

Our IT systems comply with applicable security standards and processes, including:

- access controls and passwords on key systems;
- only authorised staff are permitted remote and physical access to data centres and their devices;
- third party service providers obtain physical access to AIMS' data centres and devices under formal contract arrangements which have appropriate provisions to protect against breaches;
- specific security software is installed on all our critical IT devices;
- real-time monitoring of IT activity to detect and prevent erroneous and malicious activities;
- use of secure online payment systems; and
- encryption of electronic files where government regulations require certain personal information to be provided to other Commonwealth agencies.

We only permit limited authorised personnel to access personal and sensitive information. Access to that information is on a strict "need to know" basis only.

5. Accessing and correcting your personal information

Under the Privacy Act you have the right to ask for access to personal information that we hold about you and ask that we correct that personal information. You can ask for access or correction by contacting us and we will try to respond within 30 days. If you ask, we must give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to.

To make a request, you can either:

- send an email to privacy@aims.gov.au (this is our preferred option); or
- send hard copy correspondence to PMB 3, Townsville MC, 4810 QLD.

Requests for access to personal information relating to employment should be addressed to AIMS' Human Resources Manager. All other access requests should be directed to the Privacy Officer.

We will ask you to verify your identity before we give you access to your information or correct it, and we will try to make the process as simple as possible. If we refuse to give you access to, or correct, your personal information, we must notify you in writing setting out the reasons.

If we make a correction and we have disclosed the incorrect information to others, you can ask us to tell them about the correction. We must do so unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to associate with it (for example, attach or link) a statement that you believe the information is incorrect and why.

You may have other legal rights to request access to documents that we hold and ask for information that we hold about you to be changed or annotated if it is incomplete, incorrect, out of date or misleading. For example, you may be able to submit a request under the Freedom of Information Act. For further information see the Freedom of Information page on our website. The access and correction requirements in the Privacy Act operate alongside and do not replace other informal or legal procedures by which you can be provided with access to, or correction of, your personal information.

6. How to make a complaint

If you wish to make a complaint to us about how we have handled your personal information you should complain in writing, either:

- by email to privacy@aims.gov.au (this is our preferred option); or
- by post to PMB 3, Townsville MC, 4810 QLD, addressed to the Privacy Officer.

If we receive a complaint from you about how we have handled your personal information we will determine what (if any) action we should take to resolve the complaint. We may ask you for more information or supporting documents.

If we decide that a complaint should be investigated further, the complaint will usually be handled by a more senior officer than the officer whose actions you are complaining about.

We will tell you promptly that we have received your complaint and then respond to the complaint within a reasonable time (usually within 30 days).

If you are not satisfied with our response you may ask for a review by a more senior officer within AIMS (if that has not already happened) or you can complain to the Office of the Australian Information Commissioner.

7. How to contact us

Our most up to date contact details are available on our website at https://www.aims.gov.au/docs/about/contacts.html.

For privacy enquiries, you can contact our Privacy Officer by email to privacy@aims.gov.au or by calling (07) 4753 4444.