

Privacy Policy

About this policy

Version 2.0, July 2017

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 Office of the Australian Information Commissioner (OAIC). OAIC employees and prospective employees should also refer to our **Human resources privacy policy**. The OAIC also has a **summary privacy policy**. This policy is written in simple language. The specific legal obligations of the OAIC when collecting and handling your personal information are outlined in the *Privacy Act 1988* and in particular in the Australian Privacy Principles found in that Act. We will update this privacy policy when our information handling practices change. Updates will be publicised on our website and through our email lists.

[Back to Contents](#)

Overview

We collect, hold, use and disclose personal information to carry out functions or activities under the ***Australian Information Commissioner Act 2010*** (AIC Act), the ***Privacy Act 1988*** (Privacy Act) and the ***Freedom of Information Act 1982*** (FOI Act) and **other legislation that confer powers or functions on the OAIC** including the ***My Health Records Act 2012*** (My Health Records Act).

These functions and activities include:

- handling privacy and freedom of information (FOI) complaints and FOI reviews
- taking other regulatory action under the Privacy and FOI Act
- providing advice on privacy, FOI, and information policy issues
- consulting with stakeholders, for example, on privacy or FOI guidance
- maintaining registers, such as organisations that have opted-in to Privacy Act coverage
- responding to access to information requests
- communicating with the public, stakeholders and the media including through websites and social media
- assessing suitable candidates for career opportunities within the OAIC.

[Back to Contents](#)

Collection of your personal information

At all times we try to only collect the information we need for the particular function or activity we are carrying out.

The main way we collect personal information about you is when you give it to us. For example, we collect personal information such as contact details and complaint, review, request, data breach notification or report details when you:

- contact us to ask for information (but only if we need it)
- make a complaint about a privacy breach to us
- make a complaint about the way an agency has handled an FOI request or seek a review of an FOI decision
- ask for access to information the OAIC holds about you or other information about the OAIC's operation
- notify the OAIC about a data breach
- report a matter for investigation
- apply for a job vacancy at the OAIC.

We may also collect information from you when we investigate or review a privacy or FOI matter. If we open a file about your matter, it will often include our opinion on your matter.

We may also collect contact details and some other personal information if you are on our committees or participating in a meeting or consultation with us.

Collecting sensitive information

Sometimes we may need to collect sensitive information about you, for example, to handle a complaint. This might include information about your health, racial or ethnic origin, political opinions, association memberships, religious beliefs, sexual orientation, criminal history, genetic or biometric information.

Indirect collection

In the course of handling and resolving a complaint, data breach notification, review or an investigation, we may collect personal information (including sensitive information) about you indirectly from publicly available sources or from third parties such as:

- your authorised representative, if you have one
- applicants, complainants, respondents to a complaint, investigation, application or data breach notification or the third parties' employees and witnesses.

We also collect personal information from publicly available sources to enable us to contact stakeholders who may be interested in our work or in participating in our consultations.

Anonymity

Where possible, we will allow you to interact with us anonymously or using a pseudonym. For example, if you contact our Enquiries line with a general question 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 your name and contact information and enough information about the particular matter to enable us to fairly and efficiently handle your inquiry, request, complaint or application, or to act on your report.

Collecting through our websites

The OAIC has its own public website — www.oaic.gov.au — and we manage the **APPA** website on behalf of Asia Pacific Privacy Authorities. There are a number of ways in which we collect information through our website.

Analytics

We use Google Analytics and Piwik to collect data about your interaction with our website. We host Piwik ourselves, while Google Analytics is hosted by a third party. The sole purpose of collecting your data in this way is to improve your experience when using our site. The types of data we collect with these tools include:

- your device's IP address (collected and stored in an anonymized format)
- device screen size
- device type, operating system and browser information
- geographic location (country only)
- referring domain and out link if applicable
- search terms and pages visited
- date and time when website pages were accessed

Cookies

Cookies are small data files transferred onto computers or devices by websites for record-keeping purposes and to enhance functionality on the website.

Our website generally sets the following cookies:

- `_ga`: Google Analytics cookie
- `_pk_id.3.7ced` and `_pk_ses.3.7ced`: Piwik cookies
- `bb2_screener_`: security cookie (anti-spam)

Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please set your browser preferences to reject all cookies before accessing our website.

Email lists, registrations and feedback

We will collect information that you provide to us when signing up to mailing lists and registering for our events, or when submitting feedback on your experience with our website.

We use Vision6 to manage our mailing lists and event registrations. You can **[access the Vision6 privacy policy here](#)**.

We also utilise the services of Hotjar to collect voluntary feedback on your experience with our website. You can **[view Hotjar's privacy and data collection policies here](#)**.

Social Networking Services

We use social networking services such as Twitter, Facebook and YouTube to communicate with the public about our work. 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. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for **[Twitter](#)**, **[Facebook](#)** and **[YouTube](#)** (a Google company) on their websites.

Electronic forms

The OAIC uses the Australian Government's **[SmartForm service](#)** to enable you to, for example, lodge a complaint, application, data breach notification, enquiry or apply for a job.

When you save or submit a form using this service it is encrypted and stored in a secure server located in Australia and controlled by the Department of Industry, Innovation and Science (DIIS) until we download it. After we download a submitted form, it is deleted from that server. Saved forms that have not been submitted within the timeframe specified on the form will also be deleted from the server. We will not access or download your saved forms before you submit them unless you consent or unless there is a technical issue that requires investigation.

DIIS cannot view your information except in very limited circumstances when there is a technical issue that requires investigation. In these circumstances DIIS must seek our permission to do so.

[Back to Contents](#)

Disclosure

Common situations in which we disclose information are detailed below.

Complaints and reviews

If you make a privacy or FOI complaint, or apply for an FOI review, we will usually give a copy of the complaint or application to the respondent and, where relevant, affected third parties.

If a complainant or applicant requests that only limited information is disclosed to the respondent, we may not have enough information to be able to fairly proceed with the matter. The respondent must have sufficient information to respond to the matter in a meaningful way.

Data breach notifications

If you notify the OAIC about a data breach we will not disclose personal information about you unless you agree, or would reasonably expect us to. If the breach relates to the My Health Records Act, we may disclose your personal information to the My Health Records System Operator under s 73A of that Act.

Review of OAIC decisions

We may disclose personal information to another review body if a complainant, applicant or respondent seeks an external review of the OAIC's decision or makes a complaint to the Commonwealth Ombudsman.

Publication of decisions and reports

Generally, when we publish decisions, determinations or reports (on the OAIC website and on the [Australasian Legal Information Institute website](#)) if you are a party who is an individual we will not publish your name unless you ask for it to be published.

We may also publish other information about cases that we have resolved without a formal decision. We will not publish your name.

Disclosure to the media

We generally only provide the media with personal information relating to a complaint if you have agreed.

Disclosure to service providers

The OAIC uses a number of service providers to whom we disclose personal information. These include providers that host our website servers, manage our IT and manage our **human resources information**.

To protect the personal information we disclose we:

- 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
- 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 handle a complaint.

Disclosure to other regulators or external dispute resolution schemes

We may disclose information that relates to complaints or investigations to other Australian or international regulators, or to **external dispute resolution (EDR) schemes**. We will generally only disclose your personal information to other regulators or EDR schemes if you agree and where the information will assist the OAIC or the other regulator or EDR scheme investigate a matter.

Disclosure of personal information overseas

Generally, we only disclose personal information overseas so that we can properly handle the complaint or application. For example, if:

- the complainant or respondent to a complaint is based overseas
- an Australian-based respondent is a related body corporate to an overseas company
- you have complained to an overseas entity and the OAIC about the same or a related matter.

Web traffic information is disclosed to Google Analytics when you visit our websites. Google stores information across multiple countries.

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

[Back to Contents](#)

Quality of personal information

To ensure that the personal information we collect is accurate, up-to-date and complete we:

- record information in a consistent format
- where necessary, confirm the accuracy of information we collect from a third party or a public source
- promptly add updated or new personal information to existing records
- regularly audit our contact lists to check their accuracy.

We also review the quality of personal information before we use or disclose it.

[Back to Contents](#)

Storage and security of personal information

We take steps to protect the security of the personal information we hold from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure of that information
- taking measures to address those risks, for example, we keep a record (audit trail) of when someone has added, changed or deleted personal information held in our electronic databases and regularly check that staff only access those records when they need to
- conducting regular internal and external audits to assess whether we have adequately complied with or implemented these measures.

For further information on the way we manage security risks in relation to personal information we hold see our supplementary material on information technology security practices, below.

We destroy personal information in a secure manner when we no longer need it. For example, we generally destroy complaint records after two years, in accordance with the [**OAIC's Records Disposal Authority**](#).

Accessing and correcting your personal information

Under the Privacy Act (Australian Privacy Principles 12 and 13) 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 must 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.

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 also have the right under the FOI Act 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 further information see the [Access our information](#) page on the OAIC website.

How to make a complaint

If you wish to complain to us about how we have handled your personal information you should complain in writing. If you need help lodging a complaint, you can contact us.

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.

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 assess and handle complaints about the conduct of an OAIC officer using the **APS Values** and **Code of Conduct** and the **guidelines issued by the Australian Public Service Commission**.

We will tell you promptly that we have received your complaint and then respond to the complaint within 30 days.

If you are not satisfied with our response you may ask for a review by a more senior officer within the OAIC (if that has not already happened) or you can complain to the Commonwealth Ombudsman.

[Back to Contents](#)

How to contact us

You can contact us by:

Email:	<u>enquiries@oaic.gov.au</u>
Telephone:	1300 363 992 (from overseas +61 2 9284 9749)
Assisted Contact:	National Relay Service: TTY users phone 133 677 then ask for 1300 363 992. Speak and Listen users phone 1300 555 727 then ask for 1300 363 992. Internet relay users connect to the NRS then ask for 1300 363 992. Translating and Interpreting Service: 131 450 then ask for 1300 363 992. Apart from the local call cost these are free services for you.
Post:	GPO Box 5218 Sydney NSW 2001
Facsimile:	+61 2 9284 9666

[Back to Contents](#)

Supplementary material

OAIC information technology security practices

The Australian Human Rights Commission (the AHRC) provides information technology services to the OAIC under a Memorandum of Understanding (MOU). The AHRC is also responsible for the safe keeping and maintenance of OAIC material it holds. All of this material is stored in Australia.

In providing information technology services to the OAIC, the AHRC follows Commonwealth and industry best practice in ICT Security Management, including:

- **Commonwealth Protective Security Policy Framework**
- **Defence Signals Directorate Information Security Manual**
- **ISO/AS/NZS 31000: 2009 – Risk Management – Principles and Guidelines**
- **ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management Systems – Requirements**
- **ISO/IEC 27040:2015 – Information Technology – Security Techniques – Storage security**

For the list of mandatory requirements that cover governance, personnel, information and physical security, please visit the **Protective Security Policy Framework website**.