

**Department of Climate Change, Energy, the  
Environment and Water**

**Privacy Policy**

Complete Privacy Policy

**July 2022**

### **Change history**

Date created	v1.0 July 2022
Document owner	Head of Division, General Counsel
Date of approval	2022
Version	One

# Table of contents

---

This Privacy Policy .....	5
About this Privacy Policy .....	5
Application .....	5
Accessibility .....	5
The department's obligations under the Privacy Act .....	6
Privacy by design .....	6
The department's approach to handling personal information .....	6
What is personal information .....	6
What is sensitive information .....	6
Application to commercial information .....	7
Personal information collected by the department .....	8
Types of personal information .....	8
Remaining anonymous or using a pseudonym .....	9
How the department collects and holds your personal information .....	10
Information collected from you .....	10
Information collected from third parties .....	10
Unsolicited personal information .....	10
Methods of collection .....	10
Information handled through our website and online services .....	11
How the department holds your personal information .....	14
Storage and security .....	14
Retention and destruction of personal information .....	14
Why the department collects, holds, uses and discloses your personal information .....	15
General purposes .....	15
Health and safety .....	19
Disclosure to third parties .....	19
Overseas disclosure .....	19
Privacy Impact Assessments .....	19
How to access and correct your personal information .....	21
How to request access or a correction .....	21
How will the department consider your request .....	21
How to make a complaint or report a possible privacy breach .....	21

How to make a complaint.....	22
If you are unsatisfied with the department's response.....	22
Contact us .....	22

# This Privacy Policy

## ***About this Privacy Policy***

The Department of Climate Change, Energy, the Environment and Water (**the department**) recognises the importance of protecting your privacy and personal information. The department respects your right to privacy and complies with the [Privacy Act 1988](#) (Cth) (**Privacy Act**) in relation to handling your personal information.

This Privacy Policy tells you:

- the kinds of personal information the department may collect and hold about you and other individuals;
- how the department may collect, use, store and disclose your personal information, and for what purpose; and
- how to access and/or correct your personal information that is held by the department.

This Privacy Policy uses a 'layered policy' format, which means that it offers layers of greater or lesser detail so you can decide what is relevant to you and how much to read. If you want a snapshot of the department's personal information handling practices, you can look at the summary of our Privacy Policy available on the department's website.

This Privacy Policy is reviewed and updated annually. Any updated version will be available on the department's website.

## ***Application***

This Privacy Policy applies to the department and to APP entities which the department assists in complying with Privacy Act requirements. All references to the department in this policy includes those entities (unless the context requires otherwise).

Please contact the department if you have a query about the application of this policy, or to make comments or suggestions. Our contact details are provided at the end of this policy.

## ***Accessibility***

It is important that our information is accessible to everyone.

You can request an accessible version of this policy using the contact details provided at the end of this document.

We will take reasonable steps to provide alternate access, such as in an alternate format or language.

## The department's obligations under the Privacy Act

As an Australian Government agency, the department is bound by the Australian Privacy Principles (APPs) in the [Privacy Act](#) and the [Australian Government Agencies Privacy Code \(Privacy Code\)](#). These obligations extend to the department's employees, contractors and agents.

The Privacy Act regulates how agencies collect, use, store and disclose personal information, including sensitive information, and how individuals may access and correct personal information held about them. The Privacy Code sets out additional requirements that apply to Australian Government agencies.

You can learn more about the Privacy Act, the APPs and the Privacy Code on the website of the [Office of the Australian Information Commissioner \(OAIC\)](#) at <https://www.oaic.gov.au/>.

### ***Privacy by design***

The department has adopted a 'privacy by design' approach to managing personal information. This means embedding good privacy practices across all aspects of its functions and activities, and taking proactive steps to identify and manage privacy risks. The department achieves this by taking reasonable steps to build privacy into its business practices, workforce training, project objectives and physical infrastructures. This enables the department to ensure compliance with the APPs in an open and transparent way.

### ***The department's approach to handling personal information***

The department's approach to handling personal information is aligned with the APPs. In particular, the department:

- may collect your personal information where this is reasonably necessary for, or directly related to, one or more of its functions or activities;
- may collect your sensitive information where you consent, where the collection is authorised or required by law, or the collection is otherwise allowed under the Privacy Act;
- will only use and disclose your personal information for the purposes for which it was collected, or otherwise in accordance with the Privacy Act; and
- will notify you of the purpose that your personal information is being collected, either at the time of collection, or as soon as practicable thereafter.

### ***What is personal information***

In this Privacy Policy, the term "personal information" has the meaning given to it in the Privacy Act. "Personal information" is any information or opinion about an identified individual, or an individual that is reasonably identifiable. The information or opinion does not have to be true or recorded in a material form.

### ***What is sensitive information***

'Sensitive information' is a subset of personal information and generally has a higher level of privacy protection than other personal information.

Sensitive information is personal information that contains information or an opinion about an individual's:

- racial or ethnic origin

- political opinion or association
- religious beliefs or affiliations
- philosophical beliefs
- trade or professional associations and memberships
- union membership
- sexual orientation or practices
- criminal record
- health or genetic information; or
- certain biometric information.

***Application to business information***

Business information does not generally fall within the definition of “personal information” under the Privacy Act, but it may do so where the information relates to sole traders and partnerships. Where business information contains personal information, this Privacy Policy will apply to the personal information component.

## Personal information collected by the department

### *Types of personal information*

The department collects and holds different types of personal information to perform its functions and activities, including:

Information	Description
Personal information	<ul style="list-style-type: none"> <li>• Who you are:               <ul style="list-style-type: none"> <li>• name</li> <li>• age, birth date, gender</li> <li>• photographs, videos, audio-visual recordings</li> <li>• emergency contact details, next of kin, referee details</li> </ul> </li> <li>• Contact details:               <ul style="list-style-type: none"> <li>• mailing and/or street address</li> <li>• telephone, facsimile number, email address</li> </ul> </li> <li>• Employee, contractor and service provider information:               <ul style="list-style-type: none"> <li>• current and/or former employer, contractor and volunteer roles</li> <li>• education, training, qualifications and experience</li> <li>• hours of work, remuneration, leave records</li> <li>• current and/or past performance, disciplining</li> <li>• tax file number and superannuation fund details</li> <li>• engagement, resignation and termination</li> </ul> </li> <li>• Financial or credit information:               <ul style="list-style-type: none"> <li>• bank account and/or credit card details</li> <li>• insurance</li> </ul> </li> <li>• Licensing and approvals:               <ul style="list-style-type: none"> <li>• vessel and vehicle details</li> <li>• driver's licence, equipment licence, and other approvals/licences</li> <li>• passport and/or visa information, travel details</li> </ul> </li> <li>• The products and services you have purchased or enquired about, together with any additional information necessary to deliver those products and services and to respond to your enquiries</li> <li>• Information you give the department via our service centre, surveys, forms (hard copy and electronic), and visits by our representatives</li> <li>• Online information including information posted on our websites and social media platforms, cookie and clickstream data (this can be disabled by you), and publicly available information posted on other websites or platforms.</li> <li>• Other types of personal information as required to be collected for the purposes of the department's functions and activities.</li> </ul>



Information	Description
Sensitive information (a subset of personal information)	<ul style="list-style-type: none"> <li>• Racial or ethnic origin, such as Indigeneity when relevant to implementing the department's Reconciliation Action Plan and indigenous programs</li> <li>• Religious beliefs or sexual orientation, including where volunteered by participants in the department's diversity and inclusion network</li> <li>• Criminal records, for example as part of a national criminal history check</li> <li>• Health information, including to ensure the work, health and safety of the department's workers and other individuals.</li> <li>• Other types of sensitive information as required to be collected for the purposes of the department's functions and activities.</li> </ul>

***Remaining anonymous or using a pseudonym***

The department understands that you may not want to provide your personal information in certain situations. You may remain anonymous or use a pseudonym when dealing with the department.

However, in some circumstances, this may mean the department cannot provide the products or services you require, or the desired level of service.

Where it is impracticable or not possible for the department to deal with you anonymously or through a pseudonym, the department may ask you to identify yourself to enable the department to action your request and carry out its functions and activities.

## How the department collects and holds your personal information

### *Information collected from you*

The department will generally collect personal information directly from you. This may include:

- during your conversations with the department or its representatives via telephone or in person;
- through your written correspondence, including email and post;
- when you access and use the department's website or web-based channels, including social media platforms; and
- when you submit an application, survey or form, in hard copy or electronically.

### *Information collected from third parties*

The Privacy Act permits the department to collect your personal information from a third party if:

- you consent;
- the collection is required or authorised under an Australian law, or a court/tribunal order; or
- it is unreasonable or impracticable to collect the information directly from you.

The department may collect your personal information from third parties, including:

- persons who are authorised to act on your behalf;
- other government agencies or entities;
- institutions or industry bodies that assist with achieving the department's functions or activities;
- law enforcement and regulatory agencies;
- financial institutions and credit reporting agencies;
- contractors and service providers to the department;
- publicly available websites and online databases; and
- international bodies relevant to the department's functions or activities.

### *Unsolicited personal information*

Unsolicited personal information received by the department will be assessed and handled in accordance with the Privacy Act. If the department determines that we can lawfully retain the information, we will take reasonable steps to give you a privacy notice (or ensure you are aware of how we will use and disclose your information), unless it is impractical to do so.

### *Methods of collection*

The department collects personal information through a range of channels, including:

- telephone, facsimile and written correspondence, including paper and emails
- paper and electronic forms and surveys
- meetings
- manual and online databases and services
- department websites and web-based channels, including online portals and social media
- publicly available third party websites and web-based channels, including social media
- taped interviews, photographs and audio-visual recordings
- security vetting procedures and digital footprint checking software

- cookies, web analytics and data collection services.

At or before the time the department collects your personal information (or as soon as practicable afterwards), the department will take reasonable steps to provide you with a privacy notice (or ensure you are aware of how we will use and disclose your information), unless it is impractical to do so.

***Information handled through our website and online services***

A variety of information is handled using the department’s website, web-based channels and third party online services. Some of this may be personal information, which is summarised in the table below.

<b>Information type</b>	<b>Treatment</b>
<p>Emails and electronic forms</p>	<p>The department’s servers may record your email address if you send the department a message online. Your email address will not be added to a mailing list unless you have provided it to the department in order to subscribe to one of the department’s subscription services.</p> <p>When you send the department a message online, the department’s servers may also record your usage data in the form of page URLs that you have visited on the department’s websites. These URLs will be used for research purposes only within the department.</p> <p>Where you choose to send the department a completed electronic form that includes your personal details, the department collects personal information such as your name, address and email address. The information collected by email or electronic forms will be used only for the purpose for which you provided it, unless an exception applies.</p> <p>For those who do not wish to use the internet to transmit information, the department provides alternative ways of providing information. For example, forms may be printed (or obtained in hard copy) and lodged by post.</p>
<p>Payment information</p>	<p>If you choose to pay for a service or product using secure credit card payment facilities available on the department’s website, you will be asked to provide your credit card details. Credit card details are encrypted from the moment they are entered into an electronic form. All other information entered into an electronic form will be encrypted upon submission to the department.</p> <p>The department stores encrypted credit card details only until the industry standard charge back period has expired (currently 10 months).</p>
<p>Clickstream data</p>	<p>The department makes a record of your visits to its website and logs the following information for statistical purposes: the user's Internet Protocol (IP) address, the date and time of the visit to the site, the web pages accessed and documents downloaded, the previous site visited, and the user's web browser and operating system.</p>
<p>Google Analytics</p>	<p>In addition to web server logs, the department’s website uses Google Analytics, a web analytics service provided by Google Incorporated (<b>Google</b>). Reports obtained from Google Analytics are used to help improve the department’s website. Google Analytics uses 'cookies' to help analyse how users use the site.</p> <p>The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States of America. Google will use this information for the purpose of evaluating your use of the department’s website, compiling reports on website</p>

Information type	Treatment
	<p>activity for website operators and providing other services relating to website activity and internet usage. Google may transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google.</p> <p>By using the department's website, you consent to the processing of data about you by Google in the manner and for the purposes set out above. Please refer to <a href="#">Google's privacy policy</a> for further information.</p>
<p>Website analytics used by third party websites</p>	<p>The department may use third party platforms or websites (such as Facebook, Twitter, Campaign Monitor, LinkedIn and YouTube) to deliver or communicate content about its programs and activities.</p> <p>The sites managed by those third parties have their own privacy policies and may send their own cookies to your computer. This is different to the department's use of its own website analytics (such as Google Analytics) for evaluating how individuals use the department's websites.</p> <p>The department does not control the setting of third party cookies. The department recommends that you check the third party websites for more information about those cookies and how to manage them.</p>
<p>MailChimp</p>	<p>The department uses MailChimp to provide online tools to create, send and manage emails for the purposes of distributing department newsletters and similar communications. MailChimp may collect personal information, such as distribution lists that contain email addresses, and other information relating to those email addresses.</p> <p>For further information about the type of personal information MailChimp collects, refer to the <a href="#">MailChimp Privacy Policy</a> available at: <a href="https://www.intuit.com/privacy/statement/">https://www.intuit.com/privacy/statement/</a>.</p> <p>MailChimp is based in the United States of America (USA) and the information collected about your use of the website (including your IP address) will be transmitted to and stored by MailChimp on servers located outside Australia.</p> <p>The department is required to inform you that by subscribing to one of our email newsletters:</p> <ul style="list-style-type: none"> <li>• you consent to your personal information being collected, used, disclosed and stored as set out in MailChimp's Privacy Policy and agree to abide by MailChimp's Terms of Use;</li> <li>• you understand and acknowledge that this service utilises a MailChimp platform, which is located in the USA and relevant legislation of the USA will apply;</li> <li>• Australian Privacy Principle 8.1 contained in Schedule 1 of the Privacy Act will not apply; and</li> <li>• you understand and acknowledge that MailChimp is not subject to the Privacy Act and you will not be able to seek redress under the Privacy Act but will need to seek redress under the laws of the USA.</li> </ul> <p>You can opt out of the department's mailing list if you choose the 'unsubscribe' service provided by MailChimp in every email, or by contacting us using the contact details at the end of this policy.</p>

Information type	Treatment
	You can also disable or refuse cookies or disable Flash player; however, you may not be able to use the services provided by MailChimp if cookies are disabled.
SurveyMonkey	Where appropriate, the department collects information through SurveyMonkey, a United States-based service. Through SurveyMonkey, the department conducts surveys. SurveyMonkey adheres to its own <a href="https://www.surveymonkey.com/mp/legal/privacy/">privacy policy</a> which is available at <a href="https://www.surveymonkey.com/mp/legal/privacy/">https://www.surveymonkey.com/mp/legal/privacy/</a> .
Portals	<p><b>myGovID</b></p> <p>myGovID is administered by Services Australia and uses session-based cookies. Session based cookies are temporary cookie files transferred to your computer and erased when you close your browser. These cookies are used by myGov to allow you to perform functions within myGov once you have signed in and to gather anonymous website usage data to help improve myGov.</p> <p>myGovID does not use persistent cookies. These are cookies that remain on your hard drive until you erase them, or they expire.</p> <p>You can change your web browser setting to reject cookies, however, some functionality on the <a href="#">myGov website</a> may be affected if you reject cookies.</p> <p>For more details, please see <a href="https://my.gov.au/mygov/content/html/privacy.html">https://my.gov.au/mygov/content/html/privacy.html</a></p> <p><b>Microsoft Powerapps Portal</b></p> <p>The Powerapps Portal uses a range of different cookies for a variety of purposes. Most of these cookies are session-based cookies. For more information about the <a href="#">Powerapps Portal</a> please see: <a href="https://docs.microsoft.com/en-us/powerapps/maker/portals/admin/portal-cookies">https://docs.microsoft.com/en-us/powerapps/maker/portals/admin/portal-cookies</a></p>
Fivecast ONYX	<p>Fivecast ONYX is a cloud-based ‘software-as-a-service’ data collection and analysis platform that delivers insights from open source data.</p> <p>The department uses Fivecast to check the digital footprint of particular individuals for employment checks, security vetting, compliance and law enforcement purposes. This may occur as part of the department’s function in managing its workforce and public office holders, as well as in order to undertake the department’s administrative and statutory portfolio functions and activities.</p> <p>Fivecast may be used to review and collect publicly available information about an individual’s use of social media platforms including Facebook, Instagram, Twitter, LinkedIn and YouTube.</p> <p>Fivecast can only access information that has already been disclosed in the public domain - this may include information posted online by the individual concerned and/or their associates.</p> <p>Fivecast can only be used by authorised users and for departmental purposes.</p> <p>The <a href="#">Fivecast privacy policy</a> is available at <a href="https://www.fivecast.com/contact/privacy-policy/">https://www.fivecast.com/contact/privacy-policy/</a>.</p>

### ***How the department holds your personal information***

The department will 'hold' your personal information where it:

- physically possesses a record containing your personal information (including storage on servers owned and operated by the Department); or
- has the right or power to deal with the information, even if it does not physically possess it (such as where the personal information is stored on servers owned or operated by a third party, to which the department has access to, or in archived files).

### ***Storage and security***

The department holds personal information in a range of audio-visual, paper and electronic based records (including in cloud-based applications and services). The department complies with the Australian Government Protective Security Policy Framework for protecting departmental resources (including information) from harm or unauthorised access. Personal information is held in accordance with the collection and security requirements of the APPs, the department's policies and procedures, and the Australian Government Protective Security Policy Framework.

If personal information held by the department is lost, or subject to unauthorised access or disclosure, the department will respond in line with the OAIC's [guidance](#). The department aims to provide timely advice to affected individuals if a data breach is likely to result in serious harm.

### ***Retention and destruction***

The department will comply with all Commonwealth legal requirements in relation the retention and destruction of records containing personal information, including information management requirements in the *Archives Act 1983* (Cth). Further information is available on the [National Archives of Australia](#) website at <https://www.naa.gov.au/information-management/information-management-legislation>.

## Why the department collects, holds, uses and discloses your personal information

### General purposes

There are several general purposes for which the department may collect your personal information. The table below identifies those general purposes, and provides a short description about how the department may use and disclose that information consistent with the relevant purpose (including access restrictions). The department takes reasonable steps to ensure that personal information collected and held by it is used and disclosed on a need-to-know basis only.

Purpose of collection	Use and disclosure
<p>To manage the department’s workforce, contractors and public office holders</p>	<p>Personal information may be collected, used and disclosed as necessary to perform the department’s functions relating to the engagement, management and planning of its workforce, contractors and public office holders.</p> <p>These purposes may include undertaking activities relating to:</p> <ul style="list-style-type: none"> <li>• creating and maintaining employee records</li> <li>• identity and employment checks, and security vetting</li> <li>• recruitment, engagement, on-boarding, separation, transfer and assignment of employees, contractors and public office holders</li> <li>• ongoing security and integrity assessment, and compliance activities</li> <li>• payroll, leave, travel, training and performance management</li> <li>• emergency protocol management and business continuity planning</li> <li>• ensuring health and safety of an individual, their work colleagues, or in the workplace more generally (see below)</li> <li>• facility and asset management (including vehicles)</li> <li>• facilitating remote working arrangements (including workstation booking and set up), and related purposes.</li> </ul> <p>The department uses a desk and workforce booking system to support flexible ways of working, staff mobility and collaboration. The desk booking system uses staff names, email addresses, AGS number and the organisation unit to which staff belong.</p> <p>Personal information may be disclosed on a need-to-know basis to third parties for these purposes. This may</p>

Purpose of collection	Use and disclosure
	<p>include disclosure to departmental officers, contractors, the Australian National Audit Office, the Australian Public Service Commission, other Commonwealth agencies and entities, State/Territory government entities and overseas agencies.</p> <p>In the case of workplace investigations or compensable claims, personal information may be disclosed to Comcare, Comcover, regulatory or law enforcement agencies/advisers, and external legal advisors.</p>
<p>To provide secretariat functions to the department and independent committees, boards, panels, councils and other related bodies.</p>	<p>Personal information will be used to contact members regarding meetings, providing meeting papers, providing payments, finalising minutes on the outcomes of the meetings and other secretariat related functions.</p> <p>In some circumstances the department may share secretariat duties with other Commonwealth, State or Territory government entities. In these circumstances, personal information may be disclosed or accessed by secretariat officers from the other responsible entities on a need-to-know basis. Secretariat members' personal information may be disclosed on department, ministerial or industry body websites.</p>
<p>To communicate and consult with advisory groups, businesses, committees, individuals, panels, project taskforces and stakeholder groups.</p>	<p>Personal information will be used to communicate and consult from relevant individuals and groups. It may be disclosed to relevant third parties where necessary to achieve the outcomes of the consultation, taskforce or review.</p> <p>In limited circumstances, the department may disclose the contact details of members on a restricted database for access by members of particular interest groups.</p>
<p>Appointing and maintaining individuals to statutory authorities, accreditation programs, committees, councils and other portfolio bodies.</p>	<p>Personal information will be used and/or disclosed to decision makers (which may include external parties, including ministers, other government entities, or the chair of such committees).</p> <p>Biographical information may be disclosed on the department's website and/or in media announcements (including social media).</p>
<p>To communicate, maintain and provide information to grantees, stakeholders or other interested parties who contact the department (or the minister/parliamentary secretary) regarding applications, submissions, contracts, requests for tender and consultancies.</p>	<p>Personal information may be disclosed to third parties who implement, manage, audit or advise on the project on behalf of the department.</p> <p>Personal information may be disclosed to other government entities and officers for the purpose of administering, responding and briefing on requests etc.</p>
<p>To maintain information relating to permits, intentions, licensing, financial processes or approving applications</p>	<p>Personal information will be used for the approval of applications, licenses and requests. The decision maker will have access to any relevant personal information that is necessary to make the decision.</p> <p>Personal information may be disclosed on the department's website, databases or to other Australian</p>



Purpose of collection	Use and disclosure
	or overseas entities.
To provide stakeholders and other interested parties copies of department information, publications and newsletters.	Personal information may be disclosed to third parties who undertake mail out services on behalf of the department.
To manage, assess, evaluate and monitor department legislative compliance, policies and programs (including assistance packages, tax offsets, grants (including discretionary) and FOI requests).	<p>Personal information will be used for purposes related to the management, assessment, evaluation and monitoring activities.</p> <p>The department may disclose personal information to the Australian Tax Office, other state government departments, external bodies, consultants or related officials responsible for the assessment or oversight of grants or to evaluate the effectiveness of grants.</p> <p>The Australian National Audit Office and other potential external audit providers will undertake audits of department programs and at times this will include the disclosure of personal information.</p> <p>In line with relevant Commonwealth legislation and policy, information about successful grant recipients is published on the department's website and GrantConnect. Published information may contain personal information where the grant recipient is a sole trader or the recipient organisation has provided an individual as contact officer.</p>
To record and make payments to employees, grantees, consultants, contractors and other stakeholder groups, or to make payments to third parties on their behalf (e.g. superannuation or PAYG tax).	<p>The Tax File Number (<b>TFN</b>) is a unique identifier issued by the Commissioner of Taxation.</p> <p>The department will collect and use an individual's TFN in accordance with the Privacy Act, including to make payments to an individual (such as the payment of wages) and when reasonably necessary to verify identity.</p> <p>When collecting an individual's TFN, the department will endeavour to notify the individual:</p> <ul style="list-style-type: none"> <li>• of the taxation, personal assistance or superannuation law which authorises the department to request or collect the TFN;</li> <li>• of the purpose for which the TFN is collected and used; and</li> <li>• that declining to provide a TFN is not an offence but may result in the person paying more tax.</li> </ul> <p>Personal information (including financial information) may be disclosed to the Reserve Bank of Australia, a banking or financial institution, or a Commonwealth, State or Territory government entity where this is necessary for credit reporting, financial reporting or to make certain payments.</p>
To allow for the selection of award winners, grantees, consultancies or contractors for	Personal information will be used for the purposes of assessing successful award winners, grantees,

Purpose of collection	Use and disclosure
department programs or business.	consultancies or contractors. Personal information will generally not be disclosed outside the department.
Managing submissions and enquiries made to the department.	Personal information will be used to maintain contact information to allow for follow up or dissemination of submissions made to the department. Personal information may be published on the department's website.
To maintain information and contact details for the purposes of implementing programs administered by the department, auditing, compliance, cost recovery, regulatory purposes, leasing, levies, inspections, enforcement activities, investigations (legal / non-legal) and financial dealings.	<p>In some circumstances personal information may be published on the department's website or disclosed to third parties (private, government and statutory organisations) in line with legislation and the requirements of the Privacy Act.</p> <p>Enforcement and investigative activities may include the disclosure of personal information to other relevant Commonwealth and State based enforcement agencies, as well as the Commonwealth's legal advisors.</p>
To maintain details of academics, professionals, speakers, scientists and subject matter experts who provide advice or information to the department, or conduct training or assessment on behalf of the department on a non-ongoing basis.	In some circumstances personal information maybe be disclosed to third parties directly associated with the program's functions or when required on the department's website.
To nominate applicants for national or international awards, scholarships or fellowships.	Personal information may be disclosed to external sponsors and/or assessors and successful applicants. It may also be disclosed on the department's website or relevant websites.
To provide information or respond to any complaints, compliments or enquiries (including social media).	Personal information may be disclosed to other portfolio agencies.
To undertake research, surveys and reports of agricultural activities and businesses.	Personal information may be disclosed to other portfolio agencies and web-based data collection services such as SurveyMonkey.
To administer portfolio legislation.	Personal information may be used to administer portfolio legislation or may be disclosed to other agencies in the course of administering portfolio legislation.
To operate the department's website or functions, fulfilling requests, and to otherwise provide information, products and services.	Personal information may be disclosed to employees, contractors or service providers (including web hosting providers, IT system administrators, cloud computing services, mailing houses, couriers, payment processors, data entry service providers, electronic network administrators, debt collectors) and professional advisers (such as accountants, solicitors, business advisers and consultants).
To assist the department achieve its functions and activities, including programs falling within its portfolio responsibilities.	Personal information may be collected, used and disclosed (including to/from third parties) to enable the department to achieve its function and activities. Examples include suppliers and other third parties

Purpose of collection	Use and disclosure
	within whom the department has commercial or business relationships, marketing, research, managing grants, advisors and consultants, and related purposes and programmes.

***Workplace health and safety***

The department may collect and use the health information of its workers and contractors to ensure the health and safety of individual workers, their workplace colleagues and the workplace generally.

This includes managing potential, actual and suspected cases of COVID-19 or similar medical conditions, and may involve collecting and using personal information about a workers’ family members, or others with whom they live for that purpose.

The department may disclose health and other personal information to departmental officers on a need-to-know basis for staff management and WHS purposes. The department may also need, or be legally required to, disclose health and other personal information to other government entities or third parties, including health authorities, for health and safety purposes.

***Disclosure to third parties***

The department may disclose your personal information to third parties, where this is permitted under the Privacy Act. Those third parties include the entities or persons identified on page 10 [“Information collected from third parties”](#) and in the table above.

If the department discloses your personal information to a third party, it will take reasonable steps to ensure that the third party handles your personal information in the same manner as the department and in accordance with the APPs.

The department imposes privacy obligations on all contracting parties, including in its funding deeds, service contracts, data sharing arrangements and commercial agreements.

***Overseas disclosure***

The department may disclose personal information to overseas recipients in limited circumstances, where this is reasonably necessary, or directly related to, our work.

This may include, for example, disclosure to peer reviewers anywhere in the world where the appropriate scientific expertise exists, or to a foreign government or agency.

If it is likely that your personal information will be disclosed to an overseas recipient, we will take reasonable steps to notify you and we will only disclose the information as permitted under the Privacy Act to the overseas recipient. We will also take reasonable steps to ensure the overseas recipient treats your personal information in accordance with the APPs, such as though our contractual agreements.

***Privacy Impact Assessments***

The department is committed to undertaking Privacy Impact Assessments (PIA) for high privacy risk projects.

The Privacy Code requires that PIAs are conducted for all high privacy risk projects. Section 12(2) of the Privacy Code states that a project may be a high privacy risk project if the agency reasonably

considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

The department maintains a public register of the PIAs it conducts which is available on the department's website at [dcceew.gov.au](https://www.dcceew.gov.au).

## How to access and correct your personal information

### *How to request access or a correction*

You may request access to personal information the department holds about you at any time. You may also ask the department to update or correct your personal information if you believe it is incomplete, incorrect or misleading.

All requests must be made in writing as follows:

- Members of the public and external stakeholders - submit a request via email or letter to the relevant business area within the department. For example, applicants for a grant program should first contact the program administrator.
- Current / former employees and workforce contractors - please contact People Services Branch, or use the general contact details at the end of this policy.

If you do not know which area of the department holds your personal information, you can use the 'contact us' link on the department's website or contact details provided at the end of this Privacy Policy.

### *How will the department consider your request*

The department will consider each request on a case-by-case basis, and in accordance with the Privacy Act and other applicable legislation.

Where the department agrees to the access or correction, it will do so in the manner requested by you where this is reasonable and practicable. The department will not charge you for providing your personal information to you, or for the costs of making any corrections to your personal information. This is different to requests made under the *Freedom of Information Act 1982* (Cth).

If the department agrees to correct your personal information, it will also take reasonable steps to inform other entities of the correction (which are bound by the Privacy Act) if the department had previously disclosed your personal information to them.

The Privacy Act allows the department, in certain circumstances, to refuse access to personal information (or refuse access in the requested manner), or to refuse to make a correction. In this situation, the department will:

- provide you with a written notice including the reasons for the refusal;
- provide you with information regarding available complaint mechanisms; and,
- at your request, take reasonable steps to associate a statement with the personal information that you believe it to be inaccurate, out of date, incomplete, irrelevant or misleading.

## How to make a complaint or report a possible privacy breach

The department takes complaints seriously and treats each complaint on a case-by-case basis.

When a complaint or report of a possible privacy breach is received, the department will conduct an internal investigation. The department will take reasonable steps to acknowledge your complaint and respond within a reasonable amount of time (which is usually 30 days).

### ***How to make a complaint***

If you believe the department has breached your privacy, please contact us using the contact information below.

We will need your contact information and details of the incident so we can investigate it properly. This is best achieved if the complaint is made in writing.

Please note that if you do not provide sufficient information, the department may not be able to fully assess and respond to your complaint.

Once the department has completed its internal enquiries, you will be advised of the outcome in writing.

### ***If you are unsatisfied with the department's response***

If you are not satisfied with the department's response or how it handled your complaint, you can make a complaint to the Office of the Australian Information Commissioner (**OAIC**). Information on how to make a complaint can be found on the [OAIC website](https://www.oaic.gov.au/privacy/privacy-complaints) at <https://www.oaic.gov.au/privacy/privacy-complaints>.

You can also make a complaint to the [Commonwealth Ombudsman](https://www.ombudsman.gov.au/what-we-do/Can-we-help-you) at <https://www.ombudsman.gov.au/what-we-do/Can-we-help-you>.

## **Contact us**

If you have questions about this Privacy Policy, any concerns, or a complaint about how your privacy has been handled or a possible breach, please contact the department using one of the following options:

### **Attention: Privacy Officer - DCCEEW**

Email: [privacy@awe.gov.au](mailto:privacy@awe.gov.au)  
Postal address: GPO Box 3090, Canberra ACT 2601, Australia  
Telephone: (61 2) 6213 6000

Or use the [Contact Us](#) link on our website at [dceew.gov.au/about/contact](https://dceew.gov.au/about/contact).