Department of Agriculture

Privacy Policy

Complete privacy policy

March 2014

Change history

Date created	March 2014
Document owner	General Counsel, Office of the General Counsel
Date of approval	March 2014
Version	One

Table of contents

About this policy

The purpose of this privacy policy is to:

- clearly communicate the personal information handling practices of the Department of Agriculture (department)
- enhance the transparency of the department's operations, and
- give individuals a better and more complete understanding of the sort of personal information the department holds, and the way we handle that information.

This privacy policy has been developed to follow the 'layered policy' format, which means that it offers layers of greater or lesser detail so people can read as much as they wish and find what they need. If all you want is a snapshot of our personal information handling practices, you can have a look at our condensed privacy policy. It offers an easy to understand summary of:

- how we collect, use, store and disclose personal information, and
- how you can contact us if you want to access or correct personal information we hold about you.

If you wish to make any comments or suggestions about the privacy policy, you can do so by contacting the privacy team in the Office of the General Counsel within the department via:

Email: privacy@agriculture.gov.au
Phone: (02) 6272 3933
Mail: Privacy, Department of Agriculture, PO Box 858, Canberra ACT 2601.

Any comments and/or suggestions will be reviewed and considered by the department's privacy officers.

If you would like to request the privacy policy be made available in an alternate format or language, such as for the vision impaired, or for those from non-english speaking backgrounds, please also contact the privacy team. Reasonable steps will be taken to provide alternate access.

This privacy policy is reviewed and updated annually. Changes will be advertised via the 'Latest News' window on the department's website.

The privacy policy was last reviewed in March 2014.

Our obligations under the Privacy Act

This privacy policy sets out how we comply with our obligations under the *Privacy Act 1988* (Privacy Act). As an Australian Government agency, we are bound by the Australian Privacy Principles (APP) in the Privacy Act which regulate how government agencies collect, use, store and disclose personal information, and how individuals may access and correct personal information held about them.

Personal information

Personal information is defined in s 6(1) of the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not'.

What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances. For example, personal information could include:

- a name or address
- bank account details

- photos or videos
- information about an individual's mannerisms, their opinions or where they work.

Note: information does not have to include an individual's name to be personal information. For example, in some cases, a date of birth and post code may be enough to identify a person.

Sensitive information

Sensitive information is a subset of personal information with additional requirements under the Privacy Act.

Sensitive information is defined in the Privacy Act as information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record that is also 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/identification and biometric templates.

The kinds of personal information collected and held by the department

The department collects and holds a variety of personal information, as included in the table below.

Information Type	**Description**
Personal information	• name • age and gender • contact details (including address, phone and email addresses) • bank account details • photos, videos or audio of individuals • employment details (including occupation, qualifications, CV and remuneration) • education details (level of education, study assistance and courses) • financial information (ABN)
Sensitive information (a subset of Personal information)	• racial or ethnic origin • political opinion or association • religious beliefs or affiliations • philosophical beliefs • trade or professional associations and memberships • union membership • criminal record • health or genetic information

Dealing with the department without being identified or using a pseudonym

The APPs introduce the option for individuals to not identify themselves, or of using a pseudonym when dealing with the agency in relation to a particular matter (unless it is impracticable to do so, or the department is legally required to deal with individuals who identify themselves).

This means that in some situations when you contact the department, you do not have to identify yourself or you can use a pseudonym. These situations could include if you seek general information about a program, grant, consultation process, importing or exporting process (for example). Identification will generally only be necessary where it would be inappropriate not to identify yourself, such as if you are enquiring about the status or details of your own application for a particular program.

How the department collects and holds your personal information

How the department collects your personal information

When the department collects personal information about you, in the majority of cases, we will collect this information directly from you. However, there may be times where the department may collect personal information from your agent or a third party. If this occurs, such collection will be in accordance with the APPs.

Other entities that may collect your personal information on behalf of the department

As well as collecting personal information directly from you, the department may also collect your personal information through other individuals or organisations acting on behalf of the department, including those such as contracted service providers.

The department may also obtain personal information collected by other Australian Government agencies and State or Territory government bodies. Based on the department's functions and activities, it is most common for the department to collect personal information through, or from the following agencies or bodies (this list is not exhaustive):

- Department of Health
- Department of Human Services
- Department of the Environment
- Department of Finance
- Department of Foreign Affairs and Trade
- Department of Infrastructure and Transport
- Australian Customs and Border Protection Service
- State based health departments
- State based environment departments
- State based information departments
- Other portfolio agencies
- Industry members who assist with the certification of goods (for example, the import or export of animal, plant or biological goods)
- Contracted service providers that assist in the department's human recourses, communications or information technology functions.

Methods of collection

When the department collects personal information we may do this through using forms (either electronic or hard copy), online portals, other electronic or paper correspondence (including emails and written correspondence) and at times verbal conversations or interviews.

When the department collects your personal information, we will issue you with a privacy notice explaining the purpose of the collection, the intended use of the personal information and to whom we may disclose it.

The department collects personal information in a variety of ways, including (but not limited to):

- paper-base forms (provided by the department or printed by you)
- electronic forms (including online smart forms)
- databases
- face to face meetings
- telephone communications
- email communications
- taped interviews or audio visual recordings
- communications by fax

- departmental websites
- information provided through the department's social media sites.

The purpose of collection is important as it restricts how the department can use and disclose your personal information, unless an exception in the Privacy Act applies. This is discussed in more detail later in this privacy policy.

Unsolicited personal information

On occasion, unsolicited personal information is provided to the department by individuals (or other entities) without it being requested. The department deals with this personal information in accordance with the APP that relates to unsolicited personal information (APP 4).

Information collected through our website and online services

A variety of information is collected by using the department's website and online services. Some of this may be personal information, which is summarised in the table below:

Information type	**Treatment**
Emails and electronic forms	The department's servers may record your email address if you send us 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 our subscription services. When you send us a message online the department's servers may also record your usage data in the form of page URLs that you have visited on our websites. These URLs will be used for research purposes only within the department. Where you choose to send the department a completed electronic form that includes your personal details, the department collects personal information such as 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. 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.
Payment information	If you choose to pay for a service or product using secure credit card payment facilities available on our 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. The department stores encrypted credit card details only until the industry standard charge back period has expired (currently 10 months).
Clickstream data	The department makes a record of your visit to the 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.
Google Analytics	In addition to web server logs, the department's website also uses Google Analytics, a web analytics service provided by Google Incorporated (Google). 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. 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 our website, compiling reports on website 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. 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 Google's privacy policy for further information.

How the department holds your personal information

The department is considered to 'hold' your personal information where it:

- physically possesses a record containing your personal information, 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 by a third party, to which the department has access to, or in archived files).

The department holds personal information in a range of audio-visual, paper and electronic based records. Personal information is held on the basis that it meets the collection and security requirements of the APPs, and the department's own policies and procedures.

The department is committed to undertaking Privacy Impact Assessments (PIA) for all new and changing projects and systems in which personal information is handled. It has developed a Privacy Impact Checklist (PIC – Appendix A) which has been adopted as the department's general approach to a PIA, except in circumstances where unusually large or complex projects or systems require one.

It is departmental policy that project or system sponsors must complete the department's PIC in the planning stage of all new or changing projects or systems. Completion of the PIC identifies how personal information is sourced and flows in a project or system. It identifies the possible privacy impacts, potential problems, solutions to manage issues, and encourages good privacy practice.

Storing and securing personal information

The following policies and procedures outline how the department stores and secures personal information:

- The department's Protective Security Policy outlines the governance arrangements around information security, personal security, personnel security, physical security and security incident management.
- The department's File Maintenance and Movement Policy outlines how the department ensures information (including personal information) is managed in an efficient, uniform and accountable manner.
- The department's IT Security Policy outlines how the department holds and secures electronic information (including personal information).
- The department's Managing Documents Best Practice Guide outlines how documents (including those which contain personal information) should be treated and how to identify information which may or may not need to form part of an official record.
- The department's Need to Know Policy outlines fundamental security principles in preventing information from being misused.
- The department's Clear Desk Policy provides instructions to staff on how documents should be secured on a day to day, officer by officer basis.

- The department conducts staff training in a number of areas including risk, record keeping, information security, FOI and privacy.
- The department's Managing Emails Best Practice Guide and Email and Internet Code of Conduct policies outline how information contained in electronic information should be held, stored and secured.
- The department also implements and adheres to a number of Commonwealth standards including the Digital Transition Policy, the *Archives Act 1983* and the Defence Signals Directorate Guidelines, including the Information Security Manual.
- The department is able to monitor and review these policies and procedures through clean desk audits, security sweeps, business continuity plans and the department's fraud and risk management plan.

You can request these policies be made available by contacting the department.

Personal information held by third parties.

Under the Privacy Act the department is required to take measures to ensure that when your personal information is to be held by a third party, that the third party complies with the same privacy requirements applicable to the department.

The department has privacy clauses in all of its legal documents, including funding deeds, services contracts and various other ad-hoc arrangements. This is to ensure third parties that the department deals with are required to handle personal information in accordance with the APPs.

Retention and destruction of personal information

The department will take reasonable steps to destroy or de-identify your personal information if the department no longer needs it for the purpose it was collected, unless:

- it is contained in a Commonwealth record, or
- the department is required by law or a court/tribunal order to retain the information.

For example, if a staff member holds your personal information within emails or on a shared drive (that will not be saved on an official Commonwealth record), then they have an obligation to destroy or de-identify it once it is no longer needed for the purpose it was collected.

The purposes for which the department collects, holds, uses and discloses your personal information

The purpose for the department collecting your personal information is important as it restricts how the department can use and disclose your personal information, unless an exception in the Privacy Act applies. Unless an exception applies, the department will:

- only use or disclose your personal information for the purpose it was collected, and
- notify you of this purpose at the time of collection, or as soon as practicable after collection.

The department will only use or disclose your personal information for another purpose where it is able to do so in accordance with the Privacy Act.

There are a number of general purposes for which the department may collect your personal information. To provide further information regarding these purposes, the table below outlines the purpose for which information is typically collected, including information about how personal information is used and disclosed in accordance with that purpose. It also includes some brief information regarding how the department restricts access to your personal information.

Purpose of collection	Use and disclosure	Access
To provide secretariat functions to departmental and independent committees, boards, panels, councils and other related bodies.	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. In some circumstances the department may share secretariat duties with other Commonwealth or state based government agencies. In these circumstances, personal information will be disclosed or accessed by secretariat officers from the other responsible government agency. Secretariat members' personal information may be disclosed on relative departmental, ministerial or industry body websites.	Departmental officers within the specific secretariat team.
To communicate with advisory groups, businesses, committees, individuals, panels, projects and stakeholder groups.	Personal information will be used to communicate with individuals. It may be disclosed to relevant third parties and in some circumstances may disclose the contact details of members on a restricted database, for members of particular interest groups.	Departmental officers responsible for administration of the specific groups.
To retain information for the purpose of appointing and maintaining individuals to statutory authorities, accreditation programs, committees, councils and other portfolio bodies.	Personal information will be used and/or disclosed to decision makers (which may include external parties, including ministers or the chair of such committees). Biographical information may be disclosed on the department's website or in media announcements regarding particular appointments.	The department's appointments team and relevant business areas involved in appointments.
To maintain information relating to the employment and ongoing administration of departmental employees and public office holders.	Personal information may be disclosed to the Australian National Audit Office and Australian Public Service Commission. In rare circumstances personal information may be disclosed to overseas agencies or other Commonwealth Government entities in line with the particular officer's duties. In the case of workplace investigations or compensable claims personal information may be disclosed to Comcare, Comcover or enforcement and legal advisors.	Departmental officers responsible for the administration of personnel information.
To communicate, maintain and provide information to grantees, stakeholders or other interested parties who contact	Personal information may be disclosed to third parties who manage or maintain the project on behalf of the department.	Departmental teams responsible for the particular grant or stakeholder groups.

Purpose of collection	Use and disclosure	Access
the department (or the minister/ parliamentary secretary) regarding applications, submissions, contracts, requests for tender and consultancies.		
To maintain information details relating to permits, intentions, licensing, financial processes or approving applications for domestic, imported or exported plant, food, animal or biological goods.	Personal information will be used for the approval of applications or licenses, the decision maker will have access to the relevant personal information. Personal information may be disclosed on the department's website or to other Australian or overseas entities.	Departmental staff responsible for the particular program or authorised and restricted members of that group with access to matter specific databases or reports.
To provide stakeholders and other interest parties copies of departmental information, publications and newsletters.	Personal information may be disclosed to third parties who undertake mail out services on behalf of the department.	Departmental staff with the responsibility for distribution of requested information.
To manage, assess, evaluate and monitor departmental legislative compliance, policies and programs (including assistance packages, tax offsets, grants (including discretionary) and FOI requests).	Personal information will be used for the purposes of collection. 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. The Australian National Audit Office and other potential external audit providers will undertake audits of departmental programs and at times this will include the disclosure of personal information. In line with relevant legislation, and requirements under the Privacy Act, personal information of successful grant recipients is published on the department's website.	Departmental staff responsible for the administration and evaluation of the particular legislative compliance, policy or program.
To record and make payments to grantees, consultants, contractors and other stakeholder groups.	Personal information would usually be disclosed to the Reserve Bank of Australia to ensure payments are made.	Information of this nature is generally accessed by departmental staff who are responsible for the particular program, and those involved with payments.
To allow for the selection of award winners, grantees, consultancies or contractors for departmental programs or business.	Personal information will be used for the purposes of assessing successful award winners, grantees, consultancies or contractors. Personal information will generally not be disclosed outside the department.	Departmental staff responsible for selection and any relevant advisory panels will have access to the information needed to assist the decision of selection.
Departmental submissions.	Personal information will be used to maintain contact information to allow for follow up or dissemination of submissions	Departmental staff responsible for the program or submission.

Purpose of collection	Use and disclosure	Access
	made to the department. Personal information may be published on the department's website.	
To maintain information and contact details for the purposes of auditing, compliance, cost recovery, regulatory purposes, leasing, levies, inspections, enforcement activities, investigations (legal / non-legal) and financial dealings.	In some circumstances personal information may be published on the department's website or disclosed to third parties (private and statutory organisations) in line with legislation and the requirements of the Privacy Act. 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.	Departmental staff responsible for the particular program or actions.
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.	Departmental staff with the responsibility for these functions. Access to databases associated with maintaining personal information is only given to departmental staff on a case by case basis.
To nominate applicants for national or international awards, scholarships or fellowships.	Personal information is likely to be disclosed to external sponsors and/or assessors and successful applicants. It may also be disclosed on the department's website or relevant websites.	Departmental staff responsible for the particular application will generally have access to this personal information.
To provide information or respond to any complaints, compliments or enquiries (including social media).	Personal information may be disclosed to other portfolio agencies.	Departmental staff responsible for the collection, collation and management of survey results.
To undertake research, surveys and reports of agricultural activities and businesses.	Personal information may be disclosed to other portfolio agencies.	Department staff responsible for the collection, collation and management of a particular survey.

How to access and seek correction of your personal information

Individuals have a right to request access to their personal information and to request its correction if it is inaccurate, out of date, incomplete, irrelevant or misleading.

The department will take reasonable and practicable steps to provide you access and/or make a correction to your personal information within 30 calendar days, unless we consider there is a sound reason under the Privacy Act or other relevant law to withhold the information, or not make the changes.

If the department does not provide you access to your personal information, or refuses to correct your personal information, where reasonable we 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.

Otherwise, if the department corrects your personal information, at your request, we will also take reasonable steps to notify other agencies or organisations (bound by the Privacy Act) of the correction; if we have previously disclosed your personal information to those agencies or organisations.

If you are an external client or stakeholder you should contact the relevant business area within the department, in writing, for access to or correction of your personal information. For example, applicants for a grant program should first contact the program administrator via email or letter. If you do not know which area of the department holds your personal information you can contact the department's switch on 02 6272 3933. Alternatively, you can use the 'contact us' link on the department's website.

Current and former departmental employees who wish to gain access to, or correct their personal information need to contact the People Services Branch (HR Assist) in the first instance. HR Assist can be contacted on 02 6272 3933 or via email at HRAssist@agriculture.gov.au

How you can complain about the treatment of your personal information and how the complaint will be handled

You can make a complaint if you believe the department has breached the APPs or mishandled your personal information.

Privacy breaches can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harm to individuals, agencies and organisations. Consequently, there is no single way of responding to a privacy breach. Each breach will need to be dealt with on a case-by-case basis. All complaints and alleged breaches will be investigated by a privacy officer and the complainant will be advised of the outcome.

The department's privacy officers will investigate:

- concerns that the personal information contained in a record of a client, stakeholder or departmental officer has been mishandled
- any complaints and/or allegations about a breach of the APPs, and
- all privacy-related matters referred from the Privacy Commissioner within the Office of the Australian Information Commissioner (OAIC).

General procedures for making a privacy complaint

If you believe the department has breached the APPs or mishandled your personal information:

1. *Contact the department:* In the first instance, any privacy concerns or complaints should be reported to the department's privacy team, this can be done by email at privacy@agriculture.gov.au or via the department's telephone switch on 02 6272 3933.

2. *Submit your concern or complaint in writing*: In general, all official complaints regarding breaches or mishandling of personal information should be first made in writing to the department's privacy team, either by email at privacy@agriculture.gov.au, or post to Privacy, Department of Agriculture, PO BOX 858, Canberra ACT 2601.

3. *Reasonable amount of time:* The department will acknowledge your concern or complaint promptly upon receipt, if you provide your contact details. The department is committed to

an efficient, considered and fair resolution of concerns or complaints. All complaints are taken seriously and you can expect to be treated fairly and equitably.

4. *If you are unhappy with the department's response or reply:* You also have the option of contacting the Privacy Commissioner within the OAIC. The Privacy Commissioner can be contacted on:

   Phone: 1300 363 992
   Email: enquiries@oaic.gov.au
   Mail: OAIC, GPO Box 5218 Sydney NSW 2001

Please note: If you take a concern or make a complaint directly to the Privacy Commissioner rather than to the department in the first instance, the Privacy Commissioner may recommend you try to resolve the complaint directly with the department first.

Internal procedures for privacy breaches and/or complaints

The following table outlines the department's internal procedures for a privacy complaint and/or breach:

Stage	What Happens	Responsible Party
1.	**Contain the breach and undertake preliminary assessment** Where a formal complaint/notification has been received, privacy officers will work with the relevant business area to contain the breach and undertake a preliminary assessment of the matter. The risks and potential harm to the individual/s associated with the breach will be evaluated.	Privacy team
2.	**Notification of privacy breach** The privacy team will determine: • who needs to be made aware of the breach internally, and potentially externally • if the matter need to be reported to the department's Fraud and Security Section, and • if the individuals involved need to be notified immediately (those whose privacy has been breached) Note: matters will be escalated internally as appropriate.	Privacy team
3.	**Detailed investigation** If the preliminary assessment finds that a potentially serious breach has occurred and/or a more detailed investigation is required, the privacy team will work with the department's Integrity and Conduct Unit to investigate the matter. The investigation officer will conduct an investigation to determine: • whether the department has breached its obligations under the Privacy Act, and • where applicable, ascertain whether there has been a breach of the Australian Public Service Code of Conduct. Note: the privacy investigation may source information in a number of different ways including reviewing any associated documents and files, and undertaking interviews with departmental officers in relation to the breach. An independent investigation officer may be engaged to assist with or undertake the investigation.	• Privacy team • Integrity and Conduct Unit • Investigation Officer

Stage	What Happens	Responsible Party
4.	**Outcome of investigation** When the investigation and report have been finalised: • the department's executive will be advised of the findings, including any recommended remedial actions to help prevent future breaches, and • the complainant, client or the Office of the Australian Information Commissioner (whichever relevant) will be notified in writing of the outcome. Note: in instances where any compensation is paid, or where legal fees are incurred, the relevant line area will be expected to meet these costs.	Departmental executive
5.	**Right of review** If a complainant is not satisfied with the outcome of the department's investigation, they can complain to the Privacy Commissioner. The department must report all major privacy breaches to the Privacy Commissioner.	• Complainant • Department of Agriculture

Overseas disclosure

Before the department can disclose your personal information to an overseas recipient, it must take such steps as are reasonable to ensure ether that the overseas recipient does not breach the APPs, or that one of the following applies:

- The overseas recipient's privacy laws are at least substantially the same, or impose substantially similar standards in relation to the treatment of personal information as the Privacy Act.
- A privacy notice expressly notifies you that no steps have been taken to ensure the overseas recipient does not breach the APPs, and you have still consented to that overseas disclosure.
- The overseas disclosure is required or authorised by or under an international agreement relating to information sharing, to which Australia is a party (such as a memorandum of understanding (MoU) or information sharing treaty).
- The disclosure is authorised or required by an Australian law.
- A permitted general situation exists (as specified at section 16A of the Privacy Act).
- The department reasonably believes the disclosure is necessary for one or more enforcement related activities conducted by, or on behalf of, and enforcement body; and the recipient is a body that performs functions, or exercises powers.

Likely disclosures

In relation to some departmental functions, your personal information is likely to be disclosed to overseas recipients. The types of personal information usually disclosed include name and contact details of individuals.

Generally, personal information disclosures to overseas recipients will relate to requirements of legislation administered by the department, diplomatic functions, or enforcement activities. These disclosures are often dependent on the circumstances. For example, trade activities initiated by parties external to the department, an isolated health issue in a consignment of cattle, or an enforcement activity relating to a shipment of goods. As these types of disclosures could be made to any country, it is not practicable to create a list of those countries.

Other circumstances in which overseas disclosures are made relate to trade and biosecurity-related MoUs, international treaties or similar international functions. Some of these disclosures also depend on the circumstances so it is impracticable to list all possible disclosures.

As general guidance, the department has previously made disclosures of personal information to countries such as those in the European Union, New Zealand, Indonesia, Timor Leste, Papua New Guinea, Solomon Islands, Malaysia, Canada, and the United States of America. Although other overseas disclosures may occur in the future, it is likely that disclosures to these countries will reoccur.