Privacy, Confidentiality/Secrecy and Security Responsibilities

For Department of Human Services Agent Specified Personnel

Privacy, Confidentiality and Security Responsibilities

On 1 July 2011 Centrelink, Medicare Australia, Child Support Agency, the Family Assistance Office and CRS Australia became the Australian Government Department of Human Services (the department). The department now provides the payments and services for these organisations.

The department’s success as an organisation is founded on our integrity as a business. We must maintain a high level of government and community confidence to successfully administer these programs and provide this support into the future.

It is important that all Agent Specified Personnel have a good understanding of their privacy and security responsibilities in relation to work carried out on behalf of the department. This booklet and the associated training on privacy and security provide a good basis for developing this understanding.

In providing this service you will be handling personal information about many customers of the department. This information is provided for the purpose of performing your duties as an Agent. You are obliged to protect this information and handle it under specific rules. These rules are set down in legislation and outline the handling requirements for personal/protected information, which are detailed in this booklet.

The department must also satisfy the Commonwealth’s minimum standards of security in all aspects of its business. To achieve this, security rules relevant to your work on behalf of the department have also been documented in this booklet.

You must read this booklet and familiarise yourself with the privacy/confidentiality legislation and the department’s security policies before you begin your job as an Agent.

If you require further information about your responsibilities in relation to privacy and security please call your nominated department contact.

This booklet contains a Declaration which you must sign to be able to deliver Agent Services. In this declaration you promise to abide by the confidentiality rules detailed in this booklet.
Rules for handling personal/protected information

For the Department of Human Services (the department) to carry out its business, a large amount of sensitive personal information is collected about its customers. The community has confidence that their personal information is safe because of the department’s strong privacy culture. The foundation of this privacy culture is the department’s legal obligation to comply with the Privacy Act 1988 and the confidentiality provisions contained in the various legislation it administers, for example the Social Security (Administration) Act 1999.

Specified Personnel have an obligation to safeguard any personal information collected through the course of the business they conduct on behalf of the department.

Protected Information

Confidentiality/secrecy provisions are contained in the legislation under which the department operates, including but not limited to the following:

- Social Security (Administration) Act 1999
- Family Assistance (Administration) Act 1999
- Disability Services Act 1986
- Paid Parental Leave Act 2010
- Student Assistance Act 1973
- National Health Act 1953
- Health Insurance Act 1973
- Healthcare Identifiers Act 2010
- Aged Care Act 1997
- Dental Benefits Act 2008
- Medical indemnity Act 2002
- Midwife Professional Indemnity (Commonwealth Contribution) Scheme Act 2010
- Private Health Insurance Act 2007
- Child Support (Assessment) Act 1989
- Child Support (Registration and Collection) Act 1988

Confidentiality/secrecy provisions govern the collection, access to, use and disclosure of protected information. The confidentiality/secrecy provisions allow employees of the department to obtain, use or access protected information about customers or third parties for the purpose of performing their duties under the relevant legislation. These provisions also allow employees to disclose protected information in limited circumstances.

Protected information is generally information about a person, collected under the relevant legislation, that is or was held in the records of the department. Social security, family assistance and paid parental leave law also defines protected information to include information to the effect that there is no information about a person held in the records of the department.

A breach of confidentiality/secrecy can occur when someone views, uses, communicates, discloses, or tries to uncover protected information about a customer when it is not for the purpose of performing their functions as an employee of the department, or for another authorised purpose. It is an offence to access, use, disclose or ask for (solicit) protected information when it is not for the purpose of performing your functions as the Specified Personnel. It is also an offence to offer
to supply protected information to someone who is not authorised to receive that information. Such a breach can attract a penalty under social security or family assistance law of up to two years imprisonment. It is also an offence to offer to supply protected information to someone who is not authorised to receive that information. Information collected for the purposes of one service delivery brand (for example, the provision of Medicare services) cannot be used for the purpose of another service delivery brand (such as Child Support services) unless authorised by legislation.

To assist you in your role as the Specified Personnel we will consider how secrecy laws affect you:

- Examples
  - If a person approaches you and asks you ‘did Joe Bloggs claim a social security payment this morning?’, the fact that Joe Bloggs did or did not claim a social security payment is protected information and you cannot acknowledge either way.
  - If you need to contact a customer who is receiving Child Support services but the phone number is not on the customer’s record, you cannot access the customer’s Medicare record to obtain the phone number. This would be in breach of the secrecy provisions under the Health Insurance Act 1973.

**Personal Information**

The *Privacy Act 1988* contains the Australian Privacy Principles (APPs) which legislate the way the department collects, stores, provides access to, uses and discloses personal information of its customers and employees. The APPs are discussed in more detail below.

**Personal Information** is information or an opinion about an identified individual or an individual who is reasonably identifiable.

A breach of privacy occurs where an act or practice of an agency (e.g. the department) breaches one of the APPs in the *Privacy Act 1988* or the Tax File Number (TFN) Guidelines issued by the Privacy Commissioner. Under the Privacy Act there are no specific penalties for the individual who breaches privacy. However, Agents may have their contracts terminated if they, or their Specified Personnel, contribute to a breach of privacy.

To assist you in your role as the Specified Personnel we will consider how privacy laws affect you:

**Collection of personal information (APPs 3–5, 10)**

Personal information about customers must only be collected for the purpose of performing specific duties under the relevant legislation.

Part of your role as the Specified Personnel will be to assist customers to complete forms and make necessary enquiries about eligibility. This involves collecting personal information from customers, generally via a form and forwarding it directly to the department as soon as possible. It is not part of your role to collect records and/or lists of customers and retain them for your records. The department’s forms are developed to ensure only relevant and necessary information is collected from its customers. These forms also contain a privacy notice which advises the customer why the information is being collected, how it will be used and to whom it may be disclosed.

As Specified Personnel, you should not ask additional questions or be unreasonably intrusive when assisting a person to complete the department’s questionnaires.
Use and Disclosure of personal information (APP 6)

Specified Personnel will be required to assist customers to complete and/or accept claim forms. The information contained on these forms is ‘protected information’ and you **cannot use this information for another purpose**. Both privacy and confidentiality legislation set rules for the use of personal/protected information.

- **Examples**
  - Jenny XX comes into your office and claims Newstart Allowance. You haven’t seen her for years, and later on that day you decide it would be nice to invite her round for a barbecue with the family. You cannot use Jenny’s contact details outlined on her claim form to contact her. This is a breach of her privacy and confidentiality.
  - You run a local real estate agent’s office but also provide a service to the community as the Agent Specified Personnel. Jack XX, a Newstart customer, comes into your office and uses the computer to complete a resume and then uses the fax machine provided to fax the resume to an employer. After he leaves the office you go over to the fax machine and find the trailer which he did not collect off the machine before leaving your office. This trailer displays his current address. You realise that he was a tenant of a house you are an agent for and he left without paying the rent. You note down Jack’s current address so that you can go there after work and demand the rent owed. You cannot use his personal information for this ‘other’ purpose. This is a breach of privacy and confidentiality.

It is vital that you do NOT mix your private business with your duties as the Specified Personnel as there are severe penalties including termination of contract, for such breaches of privacy and/or confidentiality.

As the Specified Personnel, the personal information you collect from customers is protected and cannot be disclosed without authorisation.

- **Examples**
  - The local policeman approaches you as the Agent Specified Personnel and asks you for the current address of Freddie XX. He has a warrant for Fred’s arrest as he is wanted for armed robbery. Fred lodged his form earlier that morning and you remember the new address that he advised on his form. You are not authorised to divulge that address to the police officer. Tell the officer to contact the department.
  - Mrs Smith comes into your office and claims a Disability Support Pension as she has a chronic illness, forcing her to stop work at the local Service Station. You tell your friends about her illness. This is a breach of privacy and confidentiality.
  - A friend advises that his brother separated from his wife and he is not sure where she is living. His brother just wants to speak with her. You received a pension claim from the brother’s ex-wife a few weeks previously and you know her address. You are not authorised to disclose any information, including the fact that the ex-wife claimed a payment, to your friend or his brother.

You must not discuss protected/personal information about customers with third parties who are not authorised to receive this information.
Storage and Security of personal information (APP 11)

APP 11 requires the department to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. The confidentiality provisions contained in social security and family assistance law also place similar obligations on you as the Specified Personnel. This means that you must securely store the information you collect from customers. Security can refer to both physical security e.g. vaults, locks and information security.

Access to personal information (APP 12)

APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request. APP 12 also sets out other requirements in relation to giving access, including how access is to be given and when access can be refused. There are separate grounds on which agencies and organisations may refuse to give access. APP 12 operates alongside and does not replace other information or legal procedures by which an individual can be provided with access to information, including, for agencies, the Freedom of Information Act 1982 (FOI Act) that provides a right of access to information held by agencies.

Whilst the Privacy Act 1988 sets up arrangements to enable people to understand what records the department keeps, to enable people to access, alter or amend their records, self-service or the FOI Act are the preferred mechanisms used for access and amendment.

The object of the FOI Act is to provide greater access to the operations and decision-making functions of the Australian Government, particularly those that directly affect individuals.

A Freedom of Information request must be in writing, does not have to be on a departmental form and does not have to mention the words ‘freedom of information’.

If a customer requests to see information about themselves held by the department they should be advised to write a letter to the department explaining what documents they wish to see, and forward the letter to their nearest Service Centre. If the customer wants to discuss the matter, the Specified Personnel should encourage the customer to contact the department via the Smart Centre.

Physical Security

Physical Security is the first level of security for the protection of personal information you have collected on the department’s behalf. It is meant to ensure that unauthorised persons do not gain physical access to the department’s records.

Physical security in an Agent’s office could include:

- building security, such as intruder alarms and combination locks on doors;
- document security, which includes safes, lockable cabinets, secure storage and secure transportation of customer documentation.

Information Security

You must ensure that only authorised Specified Personnel access customer information and only to the extent required to do their jobs. You must not leave information about customers in a place where unauthorised persons can gain access to it. This includes other staff in your organisation who do not have a need to know this information.

- Examples
Mr Bloggs completes his claim for Age Pension, you check it, photocopy identification documents provided by him and stamp it appropriately. After Mr Bloggs leaves, you put the documents on your desk and then your partner arrives at the office to take you out to lunch. He/she picks up the claim and reads it. This is a breach of Mr Bloggs’ privacy. Completed documents should be stored securely so that they cannot be accessed by unauthorised persons.

Mrs Brown lodges with you a signed Customer Declaration Form (CDF) for Parenting Payment (Single). After she leaves your office, over morning tea, you discuss the contents of her CDF with other staff in your office who are curious as to why Mrs Brown was in the office. This is a breach of Mrs Brown’s privacy as only personnel who have a need to know to perform their duties should have access to her information.

You know that your neighbour is on Age Pension. You are curious about their circumstances because they just returned from a six month trip through the Kimberleys. You phone the department to confirm investment details. This is a breach of their privacy. You cannot make enquiries about any customer unless you are dealing with a matter on their behalf and you have their express consent. In most cases Specified Personnel would not be expected to, and should not, store confidential information on site for any period longer than is absolutely necessary. Formal means of delivery of information to the department is in place as agreed between the Agent and the host Service Centre.

The standard of storage and security is one which is reasonable in the circumstances. As Agent Specified Personnel you must exercise effective security practices to ensure the protection of information provided by customers and the provision of a secure environment wherever possible.

- It may not always be possible to provide screened interview bays, or private areas to complete forms. However, this does not mean that Specified Personnel must not strive to provide these areas.

- If a customer requests a private interview they must, where possible, be provided with one. It may be necessary to arrange an interview at a Service Centre, a home visit or contact by a Customer Service Advisor via the phone. The Specified Personnel should contact the Service Centre so appropriate arrangements can be made.

- Any information collected by the Specified Personnel should be forwarded to the department as soon as possible. If information is stored on site it must be made secure.

Conflict of Interest

Due to the very nature of working in smaller towns or communities, the role of the Specified Personnel may require them to provide services to someone they know, even family members. The Specified Personnel can continue to provide information and assistance as they do not access records or have anything to do with the processing of claims. However, if a customer is uncomfortable dealing with you as the Specified Personnel because of other dealings they have had with you (e.g. social contact, business dealings, family circumstances etc.), they should be referred to the host Service Centre or Smart Centre. This is the customer’s choice and it should be respected.

The Specified Personnel may also work for, or have an affiliation with other government agencies. In these circumstances the Specified Personnel needs to ensure that the delivery and promotion of each of these services remains completely separate both physically and in the delivery of the service. It is the responsibility of the Specified Personnel to avoid any actual or perceived conflict of interest in these circumstances.
Facsimiles
Whenever transmitting customer information via the fax machine, you must always check the fax number before sending any documentation. You must report all incidents of misdirected faxes to the department immediately.

Email
Personal information about customers must not be transmitted via email. This is not a secure environment and you must not compromise the security of confidential information.

The department is obligated under legislation to protect its assets and certain information gathered on behalf of the Commonwealth. You, as the Specified Personnel must adhere to departmental directions in these matters.

Document disposal
You should not dispose of any original department related information – all originals should be returned to the customer, or in the event they are accidentally left behind, stored securely until collection by the customer or sent to the department with an explanatory note. Copies of documents left behind may be disposed of using the department provided shredder.

Security Responsibilities
The department collects, receives and develops a substantial amount of information to fulfil its function, and expects Agents who access or hold this information to protect it.

• You must not leave personal information about customers unattended at any time. For example you should clear your desk and ensure that personal information about customers is properly secured whenever you leave your working area during the day, during short breaks (e.g. meetings or lunch) and before leaving at the end of the day.

• The availability of official information should be limited to those who need to use or access the information to do their work. Therefore, if you don’t need the information to do your work, you should not have access to it.

• You must maintain the confidentiality, integrity and copyright of all assets developed or purchased by the department. In particular, you:
  o should only use software in accordance with the approved licence agreements;
  o should not, without appropriate authority, make copies of department owned or leased assets for any purpose; and
  o should report all instances of asset misuse to your Host Service Centre Manager.

• You must ensure that all security measures and procedures are in place, to ensure that the department’s equipment, (for example computers, faxes etc.) are protected from theft, damage and unauthorised access.

• You have a duty to report all security violations, breaches and problems to your host Service Centre Manager as soon as possible, so that prompt remedial action may be taken.

• Where there is evidence of a breach of security policies, standards or procedures, an investigation will be undertaken. The outcome of such actions may result in:
o confirmation that a breach of a contractual agreement has occurred, thus initiating an internal investigation;

o confirmation that a criminal act has occurred, thus initiating a criminal investigation in conjunction with police authorities and in accordance with the Crimes Act 1914;

o relevant security awareness programs being reinforced (e.g. training, retraining); and

o security policies, standards or procedures being modified.
Privacy, Confidentiality/Secrecy and Security legislation and policy guidelines

Listed below are relevant sections contained in the following Acts:

- Social Security (Administration) Act 1999 (SSAA);
- A New Tax System (Family Assistance) (Administration) Act 1999 (FAAA); and
- Student Assistance Act 1973 (SAA).

<table>
<thead>
<tr>
<th>SSAA</th>
<th>FAAA</th>
<th>SAA</th>
<th>CONTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>201–202</td>
<td>161–162</td>
<td>351</td>
<td>Protection of personal information—who can access protected information, how it can be used and to whom it may be disclosed</td>
</tr>
<tr>
<td>203</td>
<td>163</td>
<td>352</td>
<td>Offence—unauthorised access</td>
</tr>
<tr>
<td>204</td>
<td>164</td>
<td>353</td>
<td>Offence—unauthorised use and disclosure</td>
</tr>
<tr>
<td>205</td>
<td>165</td>
<td>357–358</td>
<td>Offence—soliciting disclosure of protected information</td>
</tr>
<tr>
<td>206</td>
<td>166</td>
<td>359</td>
<td>Offence—offering to supply protected information</td>
</tr>
<tr>
<td>207</td>
<td>167</td>
<td>354</td>
<td>Protection extends to courts, tribunals, proceedings etc.</td>
</tr>
<tr>
<td>208–209</td>
<td>168–169</td>
<td>355–356</td>
<td>Secretary's certificates in relation to disclosure of information and guidelines for exercise of Secretary's power</td>
</tr>
<tr>
<td>210</td>
<td>170</td>
<td>360</td>
<td>Officer’s oath or declaration</td>
</tr>
<tr>
<td>201</td>
<td>161</td>
<td>361</td>
<td>Freedom of Information Act not affected</td>
</tr>
</tbody>
</table>

Definition of Officer

s201A of the Social Security (Administration) Act 1999 defines an 'officer' as:

(a) a person who is or has been an officer within the meaning of subsection 23(1) of the 1991 Act; or

(b) a person who is or has been appointed or employed by the Commonwealth and who, as a result of that appointment or employment, may acquire or has acquired information concerning a person under the social security law or the Farm Household Support Act 1992; or

(c) a person who, although not appointed or employed by the Commonwealth, performs or did perform services for the Commonwealth and who, as a result of performing those services,
may acquire or has acquired information concerning a person under the social security law or the *Farm Household Support Act 1992*.

**Protected Information**

The *Social Security Act 1991* defines ‘protected information’ as:

(a) information about a person that was obtained by an officer under the social security law and is or was held in the records of the Department or the Human Services Department; or

(b) information about a person obtained by an officer under the family assistance law that is or was held in the records of the Australian Taxation Office; or

(baa) information about a person that was held in the records of the Commonwealth Services Delivery Agency; or

(bab) information about a person that was obtained by an officer under the family assistance law was held in the records of Medicare; or

(bac) information about a person obtained by an officer under the family assistance law that was held in the records of the Health Insurance Commission; or

(c) information to the effect that there is no information about a person held in the records of one or more of the following:

   (i) the Department;

   (ii) the Human Services Department;

   (iii) the Australian Taxation Office.

The *A New Tax System (Family Assistance) (Administration) Act 1999* defines ‘protected information’ as:

(a) information about a person that was obtained by an officer under the family assistance law and is or was held in the records of the Department or the Human Services Department; or

(aa) information about a person that was held in the records of the Commonwealth Services Delivery; or

(b) information about a person that was held in the records of Medicare Australia; or

(ba) information about a person obtained by an officer under the family assistance law that was held in the records of the Health Insurance Commission; or

(c) information to the effect that there is no information about a person held in the records of an agency.

**Privacy legislation**

**Personal Information**

The *Privacy Act 1988* states:

‘Personal information’ means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.
Australian Privacy Principles

Part 2 – Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:
   (i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or
   (ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity’s functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:
   (i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or
   (ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or

(e) the APP entity is a non profit organisation and both of the following apply:
   (i) the information relates to the activities of the organisation;
   (ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.
Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:
   (i) the individual consents to the collection of the information from someone other than the individual; or
   (ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

4 Australian Privacy Principle 4 – Dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and
(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and
(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

5 Australian Privacy Principle 5 – notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:
(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or
(b) to otherwise ensure that the individual is aware of any such matter.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;
(b) if:
   (i) the APP entity collects the personal information from someone other than the individual; or
   (ii) the individual may not be aware that the APP entity has collected the personal information;
the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);
(d) the purposes for which the APP entity collects the personal information;
(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
(i) whether the APP entity is likely to disclose the personal information to overseas recipients;
(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.
Part 3 – Dealing with personal information

6 Australian Privacy Principle 6 – use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or
(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
   (i) if the information is sensitive information—directly related to the primary purpose; or
   (ii) if the information is not sensitive information—related to the primary purpose; or
(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or
(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and
(b) the information is biometric information or biometric templates; and
(c) the recipient of the information is an enforcement body; and
(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and
(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;
the entity must take such steps as are reasonable in the circumstances to ensure that the
information is de identified before the entity discloses it in accordance with subclause 6.1
or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph
6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:
(a) an APP entity is a body corporate; and
(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity’s primary purpose for the collection of the information
were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:
(a) personal information for the purpose of direct marketing; or
(b) government related identifiers.

Part 4 – Integrity of personal information

10 Australian Privacy Principle 10 – quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances
to ensure that the personal information that the entity collects is accurate, up to date and
complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances
to ensure that the personal information that the entity uses or discloses is, having regard
to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

11 Australian Privacy Principle 11 – security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are
reasonable in the circumstances to protect the information:
(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure.

11.2 If:
(a) an APP entity holds personal information about an individual; and
(b) the entity no longer needs the information for any purpose for which the
information may be used or disclosed by the entity under this Schedule; and
(c) the information is not contained in a Commonwealth record; and
(d) the entity is not required by or under an Australian law, or a court/tribunal order,
to retain the information;
the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5 – Access to, and correction of, personal information

12 Australian Privacy Principle 12 – access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

   (i) if the entity is an agency—within 30 days after the request is made; or

   (ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.
13 Australian Privacy Principle 13 – correction of personal information

Correction

13.1 If:
(a) an APP entity holds personal information about an individual; and
(b) either:
   (i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
   (ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:
(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and
(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:
(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and
(b) the mechanisms available to complain about the refusal; and
(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:
(a) the APP entity refuses to correct the personal information as requested by the individual; and
(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:
(a) must respond to the request:
   (i) if the entity is an agency — within 30 days after the request is made; or
(ii) if the entity is an organisation — within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

For the latest version of the Privacy Act 1988, including these principles, visit the ComLaw website: comlaw.gov.au
**Crimes Act 1914**

Section 70

This section says a Commonwealth officer must not publish or communicate any confidential or sensitive document or fact they are aware of in their capacity as a Commonwealth officer, unless it is to an authorised person. This also applies to a person who previously held a position as a Commonwealth officer.

**Criminal Code Act 1995**

This Act contains general prohibitive principles that apply to all Commonwealth public officials. The following restrictions are not exclusive and are only offered as a guide. For more information consult the Criminal Code Act 1995. In summary, this Act:

- prohibits Commonwealth public officials from destroying, stealing or intending to steal property belonging to the Commonwealth;
- has penalties against Commonwealth public officials behaving in a dishonest manner to commit or conspire to commit fraud;
- forbids a Commonwealth public official asking for, receiving or obtaining a benefit for himself, herself or another person;
- prohibits a person from intentionally and without authority obtaining access to data stored in a Commonwealth computer (This is a ‘browsing’ offence under the Criminal Code Act 1995.);
- prohibits a person damaging (destroying, erasing or altering) data held in a Commonwealth computer;
- prohibits a Commonwealth public official dishonestly using information gained in their capacity as a public official.

Penalties for breaches under this Act can range up to 10 years imprisonment.

**Government procedural standards for security**

Some procedural standards are:

- Australian Government Protective Security Manual (2007);
- Australian Communications Electronic Security Instructions (ACSI) 33;
- Gateway Certification Guide;
- Cabinet Handbook.

The Contract Delegate can assist with your privacy, confidentiality and security enquiries and show you how to access the confidentiality legislation contained within various Acts administered by the department. You can also advise them of any possible security concerns or suggestions.
Declaration of Confidentiality

I, ..............................................................................................................................................

Of ..............................................................................................................................................

hereby declare that I have been provided with the "Privacy, Confidentiality/Secrecy and Security Responsibilities for Department of Human Services Agent Specified Personnel" booklet.

I understand that this booklet details some of my privacy and confidentiality obligations and that these obligations arise under legislation.

I am aware that these obligations apply even if I am no longer the Department of Human Services Agent Specified Personnel.

I have read, understood and agree to abide by, the rules set out in this booklet.

Signature of Declarant:
Date:
..............................................................................................................................................

Witness to complete:

Declared at .................................................................................................................................

(location)

This ........................................ day of ................................................................. 20........

Before me .................................................................................................................................

(Witness Name)

..............................................................................................................................................

(Witness Signature)