

Privacy Policy



House
with No
Steps

PART A:	Summary	2
	1: What is this policy and why do we need it?	2
	2: What outcomes will be achieved by implementing this policy?	2
	3: Who does the policy affect?	2
	4: Special terms used in this policy	2
	5: Responsibilities under the policy	3
PART B:	Our Policy	4
	Annexure: Australian Privacy Principles Summary	10
PART C:	Procedures, tools & resources relevant to this policy	19

Part A: Summary

1 What is this policy and why do we need it?

- 1.1 This policy sets out how House with No Steps (HWNS) fulfils its obligations under the Privacy Act 1988 (Cth) (the Privacy Act), including the Australian Privacy Principles (APPs).
- 1.2 The APPs require HWNS to have clearly expressed policies about the management of personal information.
- 1.3 This policy outlines the type of personal information HWNS may hold and how it manages that information.

2 What outcomes will be achieved by implementing this policy?

- 2.1 People will understand their rights under the Privacy Act. This includes:
 - knowing what information HWNS holds about them;
 - information regarding the collection, use, disclosure and storage of the information; and
 - to correct that information if it is out of date or inaccurate.
- 2.2 HWNS will have in place practices, policies and procedures to make sure that the APPs are complied with, and to deal with questions and complaints about the APPs (APP1).
- 2.3 HWNS will have a clear, up to date and easy to access policy about its management of personal information (APP1). This policy is available through the HWNS website.

3 Who does the policy affect?

- 3.1 This policy applies to all of HWNS' services, activities and operations.
- 3.2 The policy affects anyone whose personal information is held by HWNS, including employees, carers, contractors, volunteers, service recipients, donors and customers.

4 Special terms used in this policy

- 4.1 For a full list of QMS definitions this section should be read in conjunction with References and Definitions.
- 4.2 "Personal Information" (as defined in the Privacy Act) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not, and whether or not the information is documented.
- 4.3 "Sensitive information" means personal information about a person's:
 - racial or ethnic origin;
 - political opinion or membership of a political association;
 - trade union or professional association membership;
 - religious beliefs or affiliations or philosophical beliefs;
 - sexual orientation or practices;
 - criminal record;
 - health information;

- genetic information; or
- biometric information or templates.

5 Responsibilities under the policy

5.1 All employees, carers, contractors and volunteers of HWNS have a responsibility to make sure personal information is handled in a way that complies with this policy.

5.2 Chief Privacy Officer: HWNS has a Chief Privacy Officer. The role of the Chief Privacy Officer is to:

- accept and answer any concerns, complaints or alleged breaches about privacy issues;
- receive and answer any requests for access to or correction of personal information; and
- be the contact for the Australian Information Commissioner in relation to any privacy issues.

Part B: Our Policy

1 Collection of Information (APP3 - 5)

- 1.1 The personal information that House with No Steps (HWNS) may request from a person will depend on the type of relationship the person has with HWNS, for example, whether the person is supported by HWNS, is an employee, carer, volunteer or donor.
- 1.2 It is HWNS' usual practice to collect personal information directly from the person.
- 1.3 Where a person is not able to provide the information, HWNS may collect the information from another person who has legal responsibility for the person.
- 1.4 HWNS allows people to have the opportunity to remain anonymous or to use a false name, except where it is not practical to do so (APP2).
- 1.5 Sometimes HWNS collects personal information from a third party or a publicly available source. This only takes place if the person has agreed to it being collected, would expect us to collect their personal information in this way or if it is necessary for HWNS to provide a service to that person.
- 1.6 HWNS only collects personal information for purposes directly related to our activities (APP3), such as:
 - providing services and support;
 - working with government and other non-government agencies;
 - operating our businesses;
 - fundraising;
 - responding to enquiries about our programs and services; and
 - administrative activities.
- 1.7 HWNS may also collect personal information in its normal communications, including when a person:
 - emails employees;
 - phones HWNS as we may store their phone number on our telephone system;
 - provides us with their business card.
- 1.8 There are some circumstances where HWNS may receive personal information that it has not asked for. When this happens, HWNS will decide whether or not we could have collected the information from that person, if we had asked. HWNS may use or disclose that information to help us make that decision (APP4).
- 1.9 If allowed to, HWNS will destroy or de-identify the information (APP4) if:
 - HWNS decides that we could not have collected the personal information if we had asked the person; and
 - the personal information is not found in a Commonwealth record.
- 1.10 HWNS does not sell, loan or give away any information that we collect.

- 1.11 Before, at the time of, or as soon as possible after HWNS collects personal information, it takes steps to tell or make sure that the person whom it is about, is aware of the following:
- who HWNS is and how to contact us;
 - the fact that HWNS has collected the information, if it was collected from someone else and how it was collected;
 - whether the collection of the information is allowed under an Australian law or a court/tribunal order;
 - the reasons why HWNS collected the information;
 - what will happen if the information is not collected;
 - whether there is anyone else that HWNS usually discloses personal information to including whether HWNS is likely to disclose the personal information to anyone overseas; and, if yes, the countries in which those people are located (APP5);
 - that HWNS' privacy policy is available and contains details regarding access and correction of the information;
 - that HWNS' privacy policy contains information about how the person may complain about a breach of the APPs, and how it will deal with any complaint.

2 Use and Disclosure of Information (APP6)

- 2.1 HWNS only holds personal information for the primary purpose it was given to us. It is not to be used or disclosed to anyone else for a secondary purpose unless one of the following applies:
- the person has agreed;
 - the person would expect HWNS to use or disclose the personal information for the secondary purpose as it relates to the primary purpose;
 - it is required or authorised by law;
 - a permitted general situation exists (see [s.16A](#) of the Privacy Act);
 - a permitted health situation exists (see [s.16B](#) of the Privacy Act), in which case, steps must be taken to de-identify the information before it is disclosed.
- 2.2 HWNS believes that the use or disclosure of the information is necessary for an enforcement related activity (e.g.: Federal Police, Immigration, ATO) (APP6).

3 Direct Marketing (APP7)

- 3.1 HWNS will not use or disclose personal information for use in direct marketing.
- 3.2 Exceptions include where a person has agreed to, or would expect HWNS to use or disclose the information for direct marketing.
- 3.3 HWNS will provide an easy way for the person to request not to receive direct marketing and will include a prominent statement that the person may make such a request.
- 3.4 A person may ask how HWNS got their information. HWNS will give them that information at no charge and within a reasonable timeframe.

5 Cross Border Disclosure (APP 8)

- 5.1 Before HWNS discloses personal information about a person to someone who is not in Australia, it will make sure that the person overseas does not breach the APPs in relation to the information.
- 5.2 Exceptions include:
- if HWNS believes that the overseas person is subject to a law that can protect the information in a way that is similar to the APPs;
 - if the person agrees to the disclosure, after being told about this APP;
 - the disclosure of the information is required by law;
 - a permitted general situation exists (see s.16A of the Privacy Act);
 - the disclosure of the information is required under an inter-Australian agreement; or
 - HWNS believes that the disclosure of the information is necessary for enforcement related activities.

6 Adoption, Use or Disclosure of Government Related Identifiers (APP9)

- 6.1 HWNS will not adopt a government related identifier of a person (e.g.: Medicare or Driver's Licence number) as its own identifier of that person unless it is allowed to do so.
- 6.2 HWNS will not use or disclose a government related identifier of a person unless:
- it is necessary for HWNS to verify the identity of the person;
 - it is necessary for HWNS to fulfil its obligations to an agency or a State or Territory authority;
 - it is required by law or a court/tribunal order;
 - a permitted general situation exists (see s.16A of the Privacy Act); or
 - HWNS believes it is necessary for an enforcement related activity.

7 Quality of Personal Information (APP 10)

- 7.1 HWNS takes reasonable steps to make sure that the personal information it collects is accurate, up to date and complete.
- 7.2 HWNS takes reasonable steps to make sure that the personal information that it uses or discloses is, considering the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.
- 7.3 These steps include maintaining and updating personal information when we are advised by a person that their personal information has changed.

8 Security of Personal Information (APP 11)

- 8.1 HWNS takes steps to protect the personal information it holds against misuse, interference, loss, unauthorised access, modification or disclosure. These steps include password protection for electronic files, securing paper files in locked cabinets and physical access restrictions.
- 8.2 When it is no longer required, personal information is destroyed, deleted or de-identified in a secure manner, unless HWNS is required by law to keep the information (APP12).

- 8.3 If a person asks for access to their personal information held by HWNS, we will allow access unless there is a reason under the Privacy Act or any other law not to give access to the information. These reasons include:
- a serious threat to the life, health or safety of any individual, or to public health/safety;
 - it would impact on the privacy of other individuals;
 - the request is frivolous or vexatious;
 - the information relates to existing or anticipated legal proceedings;
 - it would prejudice negotiations with the individual;
 - it would be unlawful;
 - denying access is authorised by law;
 - unlawful activity, or serious misconduct relating to HWNS' functions may be engaged in and giving access would prejudice the taking of appropriate action;
 - enforcement related activities may be prejudiced; or
 - evaluative information generated within HWNS in connection with a commercially sensitive decision-making process may be revealed.
- 8.4 HWNS will respond to the request for access to the personal information within a reasonable time and will give access in the way requested by the person, if it is able to do so.
- 8.5 If HWNS refuses to give access to the information or to give access in the way requested by the person, it will take steps to give access in a way that meets both its needs and those of the person, including through the use of a mutually agreed intermediary.
- 8.6 If HWNS does not agree to provide access to personal information, we will advise the person in writing of the reasons why and how to complain about the refusal.
- 8.7 There is no fee for making a request to access personal information and any fee charged by HWNS will not be excessive (e.g.: copying charges).
- 8.8 Further information about how to request access to the information we hold about a person can be obtained by contacting the Chief Privacy Officer. Further, anyone may seek advice from the Australian Information Commissioner by calling 1300 363 992 or by email: enquiries@oaic.gov.au

9 Correction (APP13)

- 9.1 HWNS will take reasonable steps to correct personal information that it holds if:
- it is satisfied that, considering the purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
 - the person requests that HWNS correct the information.
- 9.2 If HWNS corrects personal information that it previously disclosed to someone else, if requested, it will take reasonable steps to notify the other person of the correction.
- 9.3 If HWNS refuses a request to correct the personal information, it will give the person a written notice that sets out the reasons for the refusal and how they may complain about the refusal.

- 9.4 Where HWNS refuses a request to correct the personal information, the person may request that it associate or attach a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. HWNS will take reasonable steps to associate or attach the statement so that it can be seen by anyone using the information.
- 9.5 If HWNS is asked to correct personal information, it will respond within a reasonable time and will not charge the person for making the request, for making the correction or for associating the statement with the information.

10 Confidentiality

- 10.1 Employees, carers, contractors and volunteers who may have access to personal and sensitive information in the course of their duties are bound by their commitment to confidentiality.
- 10.2 Breaches of confidentiality by employees, carers, contractors and volunteers will be dealt with in accordance with the conditions of appointment of those individuals and HWNS' policy.

11 Procedures Relating to Particular Activities of HWNS

- 11.1 HWNS will develop or update its Quality Management System documentation to ensure that they comply with this policy, and to endure the effective management of personal information, including sensitive information, in the context of the broad range of its activities and operations.

12 Requesting Access or Change to Information

- 12.1 The request should be made in writing and directed to:

Chief Privacy Officer
HWNS
PO Box 93
Frenchs Forest NSW 1640
privacy@hwns.com.au

- 12.2 You should expect a response within 7 days of the request being received. You will be advised of the time it may take to provide the information, or if there is any reason why the information cannot be provided or changed in accordance with your request. If you have requested access to information, you will also be advised of how you may need to access the information.
- 12.3 Generally the information will be available free of charge, unless substantial copying is required, in which case, HWNS may request a reasonable fee to cover the cost of copying.

13 Complaints or Concerns in Relation to Privacy

- 13.1 If you have a complaint in relation to privacy, it should be made in writing, directed to:

Chief Privacy Officer
HWNS
PO Box 93
Frenchs Forest NSW 1640

- 13.2 You should expect an acknowledgement within 7 days of the complaint or concern being received. You will be advised of how your complaint or concern will be dealt with.
- 13.3 Your complaint or concern will be investigated by the Chief Privacy Officer in consultation with the Chief Executive.

- 13.4 You will receive written advice of the response to your concern or complaint, or advice of further processes required, within 28 days.
- 13.5 If HWNS' response is not acceptable to you, we may suggest conciliation or arbitration on the matter. You may also make a formal complaint to the Australian Information Commissioner by calling 1300 363 992 or by email: enquiries@oaic.gov.au

Annexure: Australian Privacy Principles Summary

Australian Privacy Principle 1 - Open and Transparent Management of Personal Information

The objective of this principle is to ensure that APP entities manage personal information in an open and transparent way.

An APP entity must:

- Take steps to implement practices, procedures and systems to:
 - ensure that it complies with the APPs; and
 - enable it to deal with inquiries or complaints regarding its compliance with the APPs.
- Have a clearly expressed and up to date policy about the management of personal information and must make the policy available.

Application to HWNS

HWNS must implement practices, policies and procedures to ensure both compliance with the APPs, and to deal with inquiries and complaints with regard to the APPs.

HWNS must have a clear, up to date and readily available policy about its management of personal information.

Questions to Consider

1. Are there any practices, procedures and systems that you need to implement in your area of business that ensures HWNS:
 - a. complies with the APPs;
 - b. adequately deals with inquiries or complaints regarding the APPs; and
 - c. makes the policy regarding the APPs available?
2. If the answer to any part of question 1 above is yes, what changes need to be made?

Australian Privacy Principle 2 - Anonymity and Pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity.

This applies unless it is not practical for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Application to HWNS

HWNS must provide anyone it deals with, with the opportunity to remain anonymous or to use a pseudonym, except where it is not practical to do so.

Questions to Consider

1. Are there changes that your area of business needs to make to ensure that people are provided with the opportunity to remain anonymous or to use a pseudonym in their dealings with HWNS?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 3 - Collection of Solicited Personal Information

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

An organisation 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 unless:
 - the individual consents to the collection of the information; and
 - the information is reasonably necessary for one or more of the entity's functions or activities; or
 - the collection of the information is required or authorised by law; or
 - a permitted general situation exists in relation to the collection of the information; or
 - a permitted health situation exists in relation to the collection of the information; or
 - the APP entity is a non-profit organisation and the information relates to the activities of the organisation and 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.

An APP entity must only collect personal information:

- by lawful and fair means; and
- from the individual unless it is unreasonable or impracticable to do so.

Application to HWNS

HWNS must only collect personal information from the individual unless it is unreasonable or impracticable to do so and if it is reasonably necessary for one or more of its functions or activities.

HWNS must only collect sensitive information with the consent of the individual; and

- when the information relates to the activities of the organisation; and
- 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.

Questions to Consider

1. Is there anything that you need to do in your area of business that ensures HWNS collects personal or sensitive information in accordance with this APP?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 4 - Dealing with Unsolicited Personal Information

If an APP entity receives unsolicited personal information, it must, within a reasonable period, determine whether or not it could have collected the information under APP 3.

The APP entity may use or disclose the personal information for the purposes of making such a determination.

If it is lawful and reasonable to do so, the APP entity is to destroy or de-identify the information if the APP entity determines that:

- it could not have collected the information under APP 3; and
- it is not contained in a Commonwealth record.

Otherwise, the information is to be treated as if it were collected under APP 3.

Application to HWNS

If HWNS receives unsolicited personal information, it is to determine whether it could have collected that information under APP 3 (in which case it may be used in accordance with the APPs), if not, it must destroy or de-identify that information.

Questions to Consider

1. Is there anything that you need to do in your area of business to ensure that, if HWNS receives unsolicited personal information, it is dealt with in accordance with this APP?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 5 - Notification of the Collection of Personal Information

Before, at the time of or as soon as practicable after an APP entity collects personal information, it must take reasonable steps to notify, or ensure that the individual is aware of, the following:

1. the identity and contact details of the APP entity;
2. the fact that the entity has collected the information, if it was collected from someone other than the individual or if the individual may not be aware that the information has been collected, and the circumstances of that collection;
3. whether the collection of the information is required or authorised by or under an Australian law or a court/tribunal order;
4. the purposes for which the APP entity collected the information;
5. the main consequences for the individual if all or some of the information is not collected;
6. whether there is any other APP entity, body or person to which the APP entity usually discloses personal information of the kind collected;
7. that the APP entity's Privacy Policy is available and contains details regarding access and correction of such information;
8. that the APP entity's Privacy Policy contains information about how the individual may complain about a breach of the APPs, and how the entity will deal with any complaint;
9. whether the APP entity is likely to disclose the personal information to overseas recipients; and, if yes,
10. the countries in which such recipients are likely to be located if it is practicable to specify those countries.

Application to HWNS

When HWNS collects personal information, it must ensure that it notifies the individual as to the matters set out at paragraphs 1 to 10 above.

Questions to Consider

1. Is there anything that you need to do in your area of business to ensure that, when you collect personal information, the individual is notified as to the matters set out at paragraphs 1 to 10 above, in accordance with this APP?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 6 - Use or Disclosure of Personal Information

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

- a. the individual has consented to the use or disclosure of the information; or
- b. one of various other exceptions apply, including:
 - expectation of use of the information;
 - requirement by law;
 - a permitted general situation exists (see [s16A](#) and [16B](#) of the *Privacy Act 1988*);
 - a permitted health situation exists (in which case, steps must be taken to de-identify the information before it is disclosed);
 - the information is required by an enforcement body (in which case, a written note must be made of the disclosure).

This APP does not apply to the use or disclosure by an organisation of personal information for the purpose of direct marketing or government related identifiers.

Application to HWNS

Prior to using or disclosing personal information that it has collected, HWNS must consider what the primary purpose was in collecting that information and what the purpose of the use or disclosure of the information is.

If the use or disclosure of the information is for a secondary purpose, then HWNS must consider whether the individual has consented to the use or disclosure of that information, and if not, whether one of the exceptions in APP 6.2 or 6.3 apply.

Questions to Consider

1. Are there any changes that you need to implement in your area of business that ensure HWNS does not use or disclose personal information for a secondary purpose, without an individual's consent?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 7 - Direct Marketing

If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Exceptions include where the individual has consented to, or would reasonably expect the organisation to use or disclose the information for that purpose, and the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications.

In each direct marketing communication, the organisation should include a prominent statement that the individual may make such a request or draw the individual's attention to the fact that they may make such a request.

An individual may request the source of the information be provided, which information must be provided at no charge and within a reasonable time.

Application to HWNS

HWNS must comply with this APP when engaging in direct marketing. In particular, it must ensure that individuals are advised as to their right to opt out of the direct marketing and that any request in this regard is acted upon in a timely manner.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which direct marketing is carried out, taking the terms of this APP into account?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 8 - Cross-Border Disclosure of Personal Information

Before an APP entity discloses personal information about an individual to a person who is not in Australia, it must take steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

Exceptions include:

- if the APP entity believes that the recipient of the information is subject to a law that can protect the information in a way that is similar to the way in which the APPs operate and there are mechanisms that the individual can access to take action to enforce that protection of the law;
- if the individual consents to the disclosure, after being informed as to the terms of this APP;
- the disclosure of the information is required by law;
- a permitted general situation exists;
- the disclosure of the information is required under an international agreement; or
- the APP entity reasonably believes that the disclosure of the information is necessary for enforcement related activities and the recipient is a body that performs functions that are similar to those performed by an enforcement body.

Application to HWNS

If HWNS is to disclose personal information to any overseas recipient, it must consider and comply with, the terms of this APP.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which you disclose personal information to overseas recipients?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 9 - Adoption, Use or Disclosure of Government Related Identifiers

An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order.

An organisation must not use or disclose a government related identifier of an individual unless:

- a. it is necessary for the organisation to verify the identity of the individual;
- b. it is necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority;
- c. it is required or authorised by or under an Australian law or a court/tribunal order;
- d. a permitted general situation exists;
- e. the organisation believes it is necessary for an enforcement related activity conducted by, or on behalf of, an enforcement body;
- f. unless prescribed by the regulations.

Application to HWNS

HWNS is to be mindful of the terms of this APP with regard to its use and disclosure of government related identifiers, such as Medicare or passport numbers.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which you use and disclose government related identifiers of individuals?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 10 - Quality of Personal Information

An APP entity must take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information that it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Application to HWNS

HWNS must take reasonable steps to ensure that the information that it collects, uses and discloses is accurate, up-to-date, complete and relevant.

Questions to Consider

1. Is there anything that you need to do in your area of business that ensures HWNS' collection, use or disclosure of personal information is accurate, up-to-date, complete and relevant?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 11 - Security of Personal Information

If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

An APP entity must take such steps to destroy information or to ensure that the information is de-identified if:

- a. the APP entity holds personal information about an individual;
- b. the APP entity no longer needs the information;
- c. the information is not contained in a Commonwealth record; and
- d. the entity is not required by law to retain the information.

Application to HWNS

HWNS must take steps to secure all personal information in its possession with regard to its misuse, interference, loss, access, modification, disclosure, destruction and de-identification.

HWNS will need to consider issues such as electronic and physical security and storage of information and documents, reviews of the use of information by its personnel, methods of destroying both physical and electronic documents etc.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which personal information is secured?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 12 - Access to Personal Information

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.

Exceptions to Access

An agency is authorised not to give access under the *Freedom of Information Act* or any other Act.

APP 12.3 sets out circumstances in which an organisation is not required to give the individual access to the personal information, including:

- a. a serious threat to the life, health or safety of any individual, or to public health/safety;
- b. it would impact on the privacy of other individuals;
- c. the request is frivolous or vexatious;
- d. the information relates to existing or anticipated legal proceedings;
- e. it would prejudice negotiations with the individual;
- f. it would be unlawful;
- g. denying access is authorised by law;
- h. unlawful activity, or serious misconduct relating to the entity's functions may be engaged in and giving access would prejudice the taking of appropriate action;
- i. enforcement related activities may be prejudiced; or

- j. evaluative information generated within the entity in connection with a commercially sensitive decision-making process may be revealed.

Dealing with Requests for Access

An organisation must respond to the request for access to the personal information within a reasonable period and give access in the manner requested by the individual, if it is reasonable and practicable to do so.

Other Means of Access

If the APP entity refuses to give access to the information or to give access in the manner requested by the individual, it must take such steps to give access in a way that meets the needs of the entity and the individual, including through the use of a mutually agreed intermediary.

Access Charges

Any charge by an organisation for access must not be excessive or apply to the making of the request.

Refusal to Give Access

If the APP entity refuses to give access, it must give the individual a written notice that sets out:

- a. the reasons for the refusal except when it would be unreasonable to do so;
- b. the mechanisms available to complain about the refusal; and
- c. any other matter prescribed by the regulations.

Application to HWNS

HWNS must comply with this APP when considering whether or not to provide access to personal information requested by an individual, including the exceptions set out at APP 12.3.

HWNS must not charge excessive fees for providing access and, where access is refused, it must provide written reasons.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which requests for access to personal information are dealt with?
2. If the answer to question 1 above is yes, what changes need to be made?

Australian Privacy Principle 13 - Correction of Personal Information

An APP entity must take reasonable steps to correct personal information that it holds if:

- it 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
- the individual requests the entity to correct the information.

Notification of Correction to Third Parties

If the APP entity corrects personal information that it previously disclosed to another APP entity, if requested by the individual, it must take reasonable steps to notify the other entity of the correction, unless it is impracticable or unlawful to do so.

Refusal to Correct Information

If the APP entity refuses a request to correct the personal information, it must give the individual a written notice that sets out the reasons for the refusal and the mechanisms for complaint about the refusal.

Request to Associate a Statement

Where the APP entity refuses to correct the personal information, as requested, the individual may request the entity associate with the information, a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

The entity must take reasonable steps to associate the statement such that it is apparent to users of the information.

Dealing with Requests

If a request is made to correct personal information, an organisation must respond within a reasonable period and must not charge the individual for the making of the request, for making the correction or for associating the statement with the information.

Application to HWNS

When considering whether or not personal information that is held by HWNS needs to be corrected, or where HWNS is requested to correct personal information, it must comply with this APP, in particular, with regard to any refusal to make the correction.

Questions to Consider

1. Are there any changes that you need to make in your area of business regarding the manner in which requests for corrections to be made to personal information are dealt with?
2. If the answer to question 1 above is yes, what changes need to be made?

Part C: Procedures, tools & resources relevant to this policy

1 List of relevant QMS Procedures & Guidelines

[References Definitions](#)

[Privacy Statement](#)

[Supported Person Files Record Establishment Policy](#)

[Incident and Continuous Improvement Reporting Policy](#)

[Complaints and Disputes Policy](#)

2 Tools and Resources for implementing this document

2.1 Legislation

Privacy Act 1988 (Cth)

Privacy Regulation 2013 (Cth)

2.2 Forms and checklists

[Privacy - Employee Acknowledgement Form](#)

[Consent for Service Form](#)

[Information Pack - Supported Persons](#)

[Consent General Media Form](#)