

# CBH SUPERANNUATION HOLDINGS PTY LTD

## AS TRUSTEE FOR

# CBH SUPERANNUATION FUND

## Privacy Policy

Date of Board approval:	12 March 2014
Next review:	March 2015
Document status:	Approved
Number of pages (incl. cover):	14

### *Policy History*

Version 4: March 2014  
Version 3: August 2013  
Version 2: February 2008  
Version 1: January 2002

This policy complies with the *Privacy Act 1988* as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

This Policy is available on the Fund's website [www.cbhsuper.com.au](http://www.cbhsuper.com.au) and a copy is available on request from the Fund Secretary.

## CONTENTS

PURPOSE .....	3
DEFINITIONS .....	3
PRIVACY OFFICER.....	3
TYPES OF INFORMATION COLLECTED AND HELD .....	4
COLLECTION AND USE OF INFORMATION.....	4
NOTIFICATION OF COLLECTION .....	5
REFUSAL TO PROVIDE INFORMATION.....	6
USE OR DISCLOSURE OF INFORMATION.....	6
ACCURACY OF INFORMATION .....	7
ACCESSING YOUR INFORMATION .....	8
DIRECT MARKETING .....	9
SECURITY OF INFORMATION .....	9
LINKS ON OUR WEBSITE .....	10
DESTRUCTION OF INFORMATION.....	10
UNSOLICITED INFORMATION .....	10
ANONYMITY.....	11
COMPLAINTS.....	11
Appendix A: Australian Privacy Principles (APPs) .....	12
Appendix B: Permitted general situations applicable to CBH Superannuation Fund.....	14

## PURPOSE

The *Privacy Act 1988* establishes requirements for organisations in dealing with personal information. From 12 March 2014, the *Privacy Act* has been amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* introducing the concept of an APP entity and Australian Privacy Principles (APPs) which replace the National Privacy Principles and Information Privacy Principles. A summary of the APPs are listed in Appendix A to this policy.

The purpose of this policy is to ensure that CBH Superannuation Holdings Pty Ltd as an APP entity and trustee for CBH Superannuation Fund manages member's personal information, fulfilling its obligations and member's rights in respect of its dealings with personal information in accordance with the *Privacy Act 1988*.

## DEFINITIONS

**APPs** is Australian Privacy Principles

**APP entity** is an agency or organisation

**The Board** is the Board of Directors of CBH Superannuation Holdings Pty Ltd

**The Fund** is CBH Superannuation Fund

**RSE Licensee** is CBH Superannuation Holdings Pty Ltd - RSE Licence No L0001625

**The Trustee** is CBH Superannuation Holdings Pty Ltd

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

**Sensitive information** is information or opinion about an individual which is:

- personal information which is also information or an opinion about the individual's racial or ethnic origins, political opinions, political association membership, religious beliefs or affiliations, philosophical beliefs, professional or trade association membership, trade union membership, sexual orientation or practices, or criminal record; or
- health, genetic or biometric information about an individual.

## PRIVACY OFFICER

The Trustee has appointed the Fund Secretary as the Fund's Privacy Officer.

The role of the Privacy Officer is to:

- provide members with information on the Privacy Policy;
- provide members, on request, with access to personal information held in regards to the individual member;
- address any member concerns regarding privacy of information;
- ensure that all Fund documents conform to privacy requirements; and
- correct personal information which is advised or found to be inaccurate.

The responsibilities of Privacy Officer are to ensure that:

- the only information collected on members is that required for superannuation purposes;
- no personal or sensitive information is provided to other parties unless required for superannuation purposes; and
- the Fund abides by its Privacy Policy.

## TYPES OF INFORMATION COLLECTED AND HELD

### Personal Information

The Trustee will collect and hold personal information that is reasonably necessary for, or directly related to, one or more of our functions or activities as the trustee of a regulated superannuation fund. This information may include (as well as other information):

- name and date of birth;
- contact details including residential address;
- employment details, employment history and salary information;
- tax file number;
- contributions history;
- nominated beneficiary details; and
- insurance claims history.

### Sensitive Information

The Trustee will only collect sensitive information (including health information) about an individual with their consent, except where we are required or permitted by law to collect their sensitive information without their consent. Sensitive information will only be collected where it is reasonably necessary for one or more of the Fund's functions or activities.

The Trustee may collect sensitive information without your consent 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. See Appendix B for permitted general situations.

## COLLECTION AND USE OF INFORMATION

The Trustee will collect and use personal information so that we can admit individuals as a member of CBH Superannuation Fund and provide them with services and benefits in connection with their membership of the Fund.

The Trustee may collect and use health information about an individual in connection with the provision of benefits, including insured benefits.

### Method of Collection

The Trustee will only collect personal information by lawful and fair means. Personal information will generally be collected directly from an individual, however information relevant to Fund membership will be collected from a member's employer where the employer makes contributions to their account.

This information will generally come from what has been provided on an application form, or through contact with an individual or their employer.

The Trustee or the Fund's insurer may collect personal and sensitive information, including health information, about an individual from third parties, such as doctors or other relevant persons, to assess and process claims for benefits, including insured benefits.

### Electronic Collection of Information

When the Trustee receives emails, it retains the content of the email and the response where it considers it necessary to do so.

A member's email address will only be used for the purpose for which it was provided, that is, for the Trustee to communicate with the member. It will not be used for any other purpose without the member's consent.

## Relevant Laws

The Trustee is subject to a variety of laws, including the *Superannuation Industry (Supervision) Act 1993* (Cth), the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and Regulations made under those Acts, which may require the Trustee to collect, hold and use information to personally identify an individual.

## Using Government Identifiers

The Trustee is required to collect and use certain government assigned identifiers, such as Tax File Numbers (TFN), when providing services for our members. The Trustee is not permitted to and does not adopt government identity numbers as if it were its own identity number.

The Trustee does not use or disclose government assigned identifiers in any way that is inconsistent with the purpose for which they were originally issued other than when authorised to or required under law. The uses that are authorised are:

- to verify the identity of the individual for the Trustee's activities or functions (such as having benefits transferred between the CBH Superannuation Fund and other superannuation funds);
- where the use or disclosure of the identifier is reasonably necessary for the Trustee to fulfil its obligations to an agency or a State or Territory authority (such as reporting contributions received for your account to the Australian Taxation Office);
- the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order;
- a permitted general situation (other than item 4 or 5 of the table) exists in relation to the use or disclosure of the identifier. See Appendix B for permitted general situations;
- the Trustee reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- the identifier is prescribed by the regulations and the Trustee is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations, and the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

## Specific Instances Relating to the Collection and Use of Information

- A member's payroll number, contributions and salary data are obtained from the member's employer. This information may be provided to the actuary, insurers, regulatory agencies or other Fund service providers on a confidential basis.
- A member's medical and personal history may be obtained in order to provide death or disability benefits and this information may be provided to the actuary or insurers in the normal course of providing such benefits.
- The *Anti Money Laundering/Counter Terrorism Financing Act* requires the Fund to establish the identity of a member before making a benefit payment. As such, the Trustee will collect identification documents (such as driver's licence, passport, birth certificate, marriage certificate) in order to be able to make benefit payments. This information may be provided to Fund service providers on a confidential basis to meet audit requirements.

# NOTIFICATION OF COLLECTION

If the Trustee collects personal information about an individual, it will at the time, or as soon as practicable afterward, notify the individual or otherwise ensure that the individual is aware:

- of the identity and contact details of the Trustee and the Fund;
- that the entity has collected the information and the circumstances of that collection;

- where 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);
- the purposes for which the Trustee collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the Trustee;
- any other APP entity, body or person (or the types of these) to which the Trustee usually discloses personal information of the kind collected;
- that the Trustee’s privacy policy contains information about how the individual may access their personal information held by the Trustee and seek the correction of their information if it is inaccurate;
- that the Trustee’s privacy policy 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 Trustee, and how the Trustee will deal with such a complaint; and
- whether the Trustee is likely to disclose the personal information to overseas recipients.

## REFUSAL TO PROVIDE INFORMATION

Any person has the right to refuse to provide the Trustee with personal information. If you decide to refuse to provide the Trustee with personal information:

- you may be unable to be admitted as a member of the Fund; or
- the Trustee may be unable to provide you with some services and benefits in connection with your membership of the Fund.

There may be other consequences relating to the type of information that you refuse to provide.

### Specific Instances Relating to a Refusal to Provide Information

- If a member refuses provide their tax file number, the Trustee may reject their application to join the Fund or if membership is accepted, the Trustee will be unable to accept personal after-tax contributions for their account and additional tax deductions may be made from contributions made by their employer, including salary sacrifice contributions.
- If a member refuses to provide medical information, the Trustee will be not provide insured death or disability benefits for the member, other than any insurance which they were granted under automatic acceptance provisions by the insurer.
- If a member refuses to provide medical information, the Trustee will not be able to assess a claim for insured disability benefits for the member.

## USE OR DISCLOSURE OF INFORMATION

In general, the Trustee will not use or disclose personal information for any purpose other than the purpose for which it was given (the primary purpose).

The Trustee may use or disclose the information for another purpose if:

- you have consented to the use or disclosure of the information for that other purpose;
- you would reasonably expect the Trustee to use or disclose the information for the other purpose and the other purpose is:
  - i. directly related to the primary purpose (if the information is sensitive information); or
  - ii. related to the primary purpose (if the information is not sensitive information);
- the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;

- a permitted general situation exists in relation to the use or disclosure of the information by the Trustee; See Appendix B for permitted general situations; or
- the Trustee 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.

The Trustee may disclose personal information to other organisations, for example, to:

- the Fund's insurer in order for insured benefits to be provided;
- a member's employer, if they are an employer-sponsored member;
- other superannuation trustees;
- external service providers, such as auditors, lawyers and mailing houses;
- government or regulatory authorities, where required or permitted by law.

The Trustee will take all reasonable steps to ensure that these organisations are bound by confidentiality and privacy obligations with respect to the protection of personal information before any personal information is disclosed to the organisation.

The Trustee is unlikely to disclose personal information to any overseas recipients.

### **Specific Instances Relating to Disclosure of Information**

- The Trustee will not add a member's email address to any external mailing lists.
- Member information will be provided to financial planners, accountants, taxation agents or similar parties only with the consent of the member.
- A member's spouse or ex-spouse will be provided with member account details in accordance with Family Law Act requirements upon receipt of a request for superannuation information accompanied by a properly completed Form 6 Declaration.
- Information will be provided to statutory agencies such as Centrelink only after they have established that they have a legal right to obtain such information.
- Information will be provided in industry surveys or similar forums only when member identification can be protected.

## **ACCURACY OF INFORMATION**

The Trustee takes reasonable steps to make sure the personal information collected, used or disclosed is accurate, up-to-date, complete and relevant. Where the Trustee believes that the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading, it will take reasonable steps to correct that information.

You may request that the Trustee corrects the personal information held for you by contacting the Fund Secretary. The Trustee will take reasonable steps to correct the information to ensure that it is accurate, up-to-date, complete, relevant and not misleading.

The Trustee will deal with a request to correct personal information within a reasonable time.

If the Trustee has previously disclosed personal information about a member to another entity and it is corrected, the Trustee will advise the other entity of the correction if the member requests it to do so unless it is impracticable or unlawful to do so.

If the Trustee does not agree with the corrections requested, it is not obliged to alter your personal information. However, where the Trustee refuses a request to correct personal information, a written notice will be given to you advising the reason(s) for the refusal and the mechanisms available to complain about the refusal.

If the Trustee refuses to correct your personal information as requested, you can request the Trustee to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. The Trustee will 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.

The Trustee will not charge you for the making of the request, for correcting the personal information or for associating a statement with the personal information.

### **Specific Instances Relating to Accuracy of Information**

- The Trustee may require proof of correct personal details if it can not verify from documents held that the information is inaccurate. For example if a member's name, date of birth or Tax File Number matches the details provided on the application form or other documents previously received, the Trustee will require proof of the correct details if the member subsequently claims their details are inaccurate.
- If a member has changed their name, the Trustee will update records only after receipt of proof of change of name such as a copy of the marriage certificate or Change of Name certificate.

## **ACCESSING YOUR INFORMATION**

Members have the right to full access to their complete superannuation file and details, subject only to identification and normal convenience issues. This can be done by forwarding a request in writing to the Trustee or contacting the Fund Secretary to make an appointment.

The Trustee will not generally charge for giving access to personal information, however it reserves the right to charge a reasonable amount as reimbursement for costs incurred by the Trustee in giving access.

The Trustee will deal with your request for such access within a reasonable time and in the manner you request if it is reasonable and practicable to do so.

### **Refusing Access**

The Trustee may refuse access if:

- the Trustee 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;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the Trustee and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the Trustee in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- the Trustee 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 and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or



- giving access would reveal evaluative information generated within the Trustee in connection with a commercially sensitive decision-making process.

If the Trustee believes it should refuse access, you will be provided with a written notice which sets out the reasons for the refusal, the relevant provisions of the Privacy Act that was relied on to refuse access and the mechanism available to complain about the refusal.

If the Trustee refuses to give access in the manner you request, it will take such steps as reasonable to give access in a way that meets the needs of the Trustee and you. This may include access being given through the use of a mutually agreed intermediary.

## **DIRECT MARKETING**

The Trustee will not generally use or disclose any personal or sensitive information held for the purpose of direct marketing. The Trustee will not add a member's email address to any external mailing lists or provide personal information to any external organisation for the purpose of direct marketing.

The Trustee will use personal information about you for the purpose of direct marketing only if:

- the Trustee collected the information from you and you would reasonably expect the Trustee to use or disclose the information for direct marketing; or
- you have consented to the use or disclosure of the information for that purpose.

The Trustee will only use or disclose your sensitive information for the purpose of direct marketing if you have consented for it to do so.

If the Trustee does send direct marketing communications, it will include a prominent statement advising the simple means for you to easily request not to receive direct marketing communications from the Trustee. If you make such a request, your personal information will no longer be used for this purpose.

## **SECURITY OF INFORMATION**

The Trustee holds personal information in paper-based and electronic files and takes all reasonable steps to ensure that personal information held is protected from:

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

In respect of paper-based files, the Trustee maintains various security systems on its premises, and in respect of its electronic files, it maintains secure electronic network systems.

### **Member communications**

The normal business of superannuation involves providing members with details of their account.

For current employee members, documents which may contain personal information may be sent in sealed envelopes to the member's work location through the Company's internal mail. Information may also be sent to a member's postal or e-mail address.

For member's who are not current employees, information will be sent to the member's postal or e-mail address.

The Fund will not use facsimile machines to transmit personal information to a member unless specifically requested by the member to do so.

Personal information will only be provided over the telephone when the Fund Secretary has established the caller's identity by the caller providing information likely only to be known by the member.

Where identification of a telephone caller can not be established, the Trustee will provide the requested information in written form to the member's work, residential or e-mail address.

### **Website Security**

The security of personal information accessible on the internet requires you to take specific measures to protect against unauthorised access or use. These include:

- that you do not divulge your password to anyone;
- ensuring your login name and passwords are kept secure; and
- notifying us immediately if you believe that your passwords have been breached.

The Trustee makes reasonable efforts to ensure that the most up-to-date security measures are used on its website to protect member's personal information. However, it cannot guarantee that any information that can be accessed through its website is entirely secure. Members should be aware that they use the website at their own risk.

### **Collection of information on website**

When you browse our website, our service provider stores the following information:

- the date and time of your last website visit;
- your recently used passwords (these are encrypted);
- the pages you accessed; and
- if you ran any reports, that a report was run, but not the parameters used for the report.

We may use this data to analyse usage patterns so that we can ensure our website content meets our member's needs, however no individual or their browsing activities will be identified.

## **LINKS ON OUR WEBSITE**

Our website [www.cbhsuper.com.au](http://www.cbhsuper.com.au) may contain links to third party websites. The Trustee advises that the terms of this Privacy Policy do not apply to external websites.

If you wish to find out how any third parties handle your personal information, you will need to obtain a copy of their privacy policy.

## **DESTRUCTION OF INFORMATION**

The current Trustee policy is to retain member records for 10 years following the member's departure from the Fund.

When the Trustee no longer requires personal information for a member (including when it is no longer required by law to keep records relating to a member), the Trustee will ensure that the personal information is destroyed or de-identified.

## **UNSOLICITED INFORMATION**

If the Trustee receives personal information about an individual that we have not requested, and we determine that we couldn't have lawfully collected that information under Privacy law if we had requested it, we will destroy or de-identify the information, if it is lawful and reasonable to do so.

If the Trustee determines that it could have lawfully collected the personal information, it will deal with the information as outlined in this policy as if it had solicited the information.

## ANONYMITY

The Trustee understands that anonymity can play an important part in privacy and that some people may wish to have the option of not identifying themselves when dealing with the Fund. Unless there is a good practical or legal reason to identify someone, the Trustee will allow individuals to remain anonymous when dealing with the Trustee in relation to generic information about the Fund.

You should note, however, that membership of the Fund requires the Trustee to obtain personal information. Should you refuse to provide identifying information, the Trustee may not be able to provide you with membership in the Fund.

The Trustee may also not be able to give specific information to you about your account or your situation if you wish to remain anonymous.

## COMPLAINTS

Any complaints about the Privacy Policy or the use of member's information should be addressed to the Fund's Privacy Officer. Your complaint will be acknowledged within 2 business days of receipt and will generally be dealt with within 28 days.

All complaints will be brought to the attention of the Fund Trustee.

If you are unsatisfied with the resolution of the complaint you make to the Fund, you can refer the matter to the Privacy Commissioner. The contact details for the Office of the Privacy Commissioner are as follows:

Office of the Privacy Commissioner

GPO Box 5218

SYDNEY NSW 2001

Phone: 1300 363 992

Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

Website: <http://www.oaic.gov.au/privacy/making-a-privacy-complaint>

## **Appendix A: Australian Privacy Principles (APPs)**

### **Part 1 - Consideration of personal information privacy**

#### ***APP 1 - open and transparent management of personal information***

Entities must manage personal information in an open and transparent way.

#### ***APP 2 - anonymity and pseudonymity***

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity in relation to a particular matter.

### **Part 2 - Collection of personal information**

#### ***APP 3 – collection of solicited personal information***

Entities 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.

Entities must not collect sensitive information about an individual unless the individual has consented to the collection and the information is reasonably necessary for one or more of the entity's functions or activities.

#### ***APP 4 – dealing with unsolicited personal information***

If an entity receives personal information that it did not solicit and determines that they could not have collected the information under APP 3, the entity must as soon as practicable destroy the information or ensure that the information is de-identified.

#### ***APP 5 – notification of the collection of personal information***

Where an entity collects personal information about an individual, it must ensure the individual is notified or aware of the identity of the entity and that they have collected the information.

### **Part 3 – Dealing with personal information**

#### ***APP 6 – use or disclosure of personal information***

Where an entity has collected personal information for a particular purpose, the entity must not generally use or disclose the information for another purpose unless the individual has consented to the use or disclosure for the other purpose.

#### ***APP 7 – direct marketing***

Entities generally must not use or disclose personal information held about an individual for the purpose of direct marketing.

#### ***APP 8 – cross-border disclosure of personal information***

Before an entity can disclose personal information about an individual to an overseas recipient, generally the entity must ensure the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

***APP 9 – adoption, use or disclosure of government related identifiers***

Entities must not adopt a government related identifier of an individual as its own identifier of the individual unless required or authorised by law.

Entities generally must not use or disclose a government related identifier unless it is necessary to verify the identity of the individual or fulfil its obligations to a government agency or authority.

**Part 4 – Integrity of personal information**

***APP 10 – quality of personal information***

Entities must ensure that the personal information that the entity collects, uses or discloses is accurate, up to date and complete.

***APP 11 – security of personal information***

Entities must protect personal information from misuse, interference and loss and unauthorised access, modification and disclosure.

Entities must ensure that if they hold personal information and no longer need the information, they destroy the information or ensure it is de-identified.

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

***APP 12 – access to personal information***

Entities must generally give an individual access to their personal information on request.

***APP 13 – correction of personal information***

Entities must correct personal information if requested to by the individual or if the entity is otherwise satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading.

## Appendix B: Permitted general situations applicable to CBH Superannuation Fund

Under section 16A of the Privacy Act

- (1) A **permitted general situation** exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:
- (b) the item in column 2 of the table applies to the information or identifier; and
  - (c) such conditions as are specified in the item in column 3 of the table are satisfied.

Item	Column 2 Item applies to	Column 3 Condition(s)
1	(a) personal information; or  (b) a government related identifier.	(a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	(a) personal information; or  (b) a government related identifier.	(a) 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; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	Personal information	(a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and  (b) the collection, use or disclosure complies with the rules made under subsection (2).
4	Personal information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
5	Personal information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

- (2) The Privacy Commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table above.