PRIVACY POLICY

Reviewed August 2016

Brien Holden Vision Institute,
Public Health Division
## TABLE OF CONTENTS

**Privacy Policy**
- Privacy Officer Contact Details  p 1
- Staff Responsibilities  p 1
- Scope and Objectives  p 1
- Complaints Handling  p 2
- Contact Database  p 2
- Administration and Employee Records  p 2
- Activities  p 2

**Privacy Principles Summary and Implementation**  p 3

**Appendix A**
- Privacy Checklist  p 9

**Appendix B**
- Website Privacy Statement  p 10
Privacy Policy

The Brien Holden Vision Institute Foundation (ABN 86 081 872 586) (also known as the Public Health Division of the Brien Holden Vision Institute and hereinafter referred to as “the Institute”) is committed to protecting the privacy of individuals and compliance with the 13 Australian Privacy Principles as set out in the Privacy Act 1988 (Cth) (hereinafter referred to as “the Act”).

The Institute has prepared this Policy to:
   a) describe the manner and circumstances under which personal information (as defined in the Act) is collected, stored, used and disclosed by the Institute;
   b) set out how an individual can access and correct any personal information held by the Institute about that individual; and
   c) outline a process for how a privacy complaint can be made and will be dealt with by the Institute.

The Policy is intended as a guide to the directors, officers, employees, staff, contractors, agents, volunteers, students, and any other person that may be authorised by, or who may have access to, any personal information collected or held by the Institute (“Personnel”), and/or will be made available to the Institute’s clients, patients or any person in the broader community on request.

The Act includes a set of 13 Australian Privacy Principles (“APPs”) that aim to ensure that organisations handle information about people responsibly. The APPs also give people more control over the way that information about them is handled.

The Institute will provide a copy of this Policy and give appropriate training to all Personnel handling personal information.

All Personnel are required to comply with this Policy.

Further information on the Privacy Act can be found on the website of the Office of the Australian Information Commissioner at www.oiac.gov.au

Privacy Officer Contact Details

Any enquiries regarding this Policy should, in the first instance, be directed to the Institute’s Privacy Officer, who may be contacted as follows:

Mail: The Privacy Officer
      Brien Holden Vision Institute, Public Health Division
      Level 4, North Wing, Rupert Myers Building
      Gate 14, UNSW, Barker Street, Sydney, NSW
      Australia 2052

Telephone: +61 2 9385 7516
Facsimile: +61 2 9385 7401
Email: privacy@brienholdenvision.org

Staff Responsibilities

It is the responsibility of management to inform Personnel of the Privacy Policies and Procedures that are established, maintained and enforced by the Institute. Management must also ensure that they periodically advise Personnel of any changes or any new Privacy Policies and Procedures in a timely manner.

All Personnel are responsible for ensuring that they understand and adhere to all Privacy Policies and Procedures implemented by the Institute, and that they maintain up-to-date knowledge of any changes or
any new Privacy Policies or Procedures. All Personnel also have a responsibility to maintain the confidentiality of all personal information that they have access to at the Institute.

At no times will ignorance of the existence of any Privacy Policies or Procedures be an acceptable excuse for non-compliance.

Scope and Objectives

The Privacy Policies and Procedures implemented by the Institute extend to and cover all operations and functions of the organisation. All Personnel must abide by these Privacy Policies and Procedures.

The objectives of these Privacy Policies and Procedures are to ensure that a sound privacy foundation and framework is established and maintained by the Institute.

(Privacy Policies are defined as the broad statements describing required privacy objectives and incorporate the ‘Australian Privacy Principles’. Privacy Procedures are defined as the measures intended to ensure that the Privacy Policies or objectives are properly met.)

Complaints Handling

Any complaints in relation to the Institute’s handling of personal information should be directed to the Privacy Officer. In most cases the complainant will be asked to lodge their complaint in writing.

Unless the complaint can be dealt with immediately to the satisfaction of both parties, the Institute will provide a written response to the complaint with 30 days of it being received.

If an individual believes their complaint has not been appropriately handled by the Institute, or if the Institute is unable to resolve the complaint, the Institute may ask the individual to participate in a dispute resolution process (such as mediation). The individual may also take the complaint to the Office of the Australian Information Commissioner (“OAIC”) by calling 1300 363 992 (local call charge) or logging on to the OAIC website at www.oaic.gov.au.

Contact Database

The Institute currently holds contact information in an access-restricted database. The Institute database has a DO NOT MAIL field in which the OPT OUT option from any contact can be recorded. This will result in no mail at all being sent to that contact.

Administration and Employee Records

All personal information concerning Institute Personnel is held by the Institute in accordance with relevant existing Industrial Relations and Employee legislation.

Applicants providing personal information to the Institute for consideration in relation to an offer of employment or other engagement, whether or not solicited by the Institute, will have their personal information handled in accordance with the APPs and kept confidential at all times with access to that personal information granted only to Personnel requiring that information to consider whether to offer the applicant employment with or other engagement by the Institute. Unless the Institute obtains permission to store an applicant’s personal information, the personal information of any unsuccessful applicants will be destroyed in a secure way at the end of the process.
Activities

All activities carried out by the Institute staff involving the collection of an individual’s personal information are also subject to the APPs.

In each case, the relevant Institute Personnel will consider the APPs in planning what information is collected, how it will be stored securely and what it will be used for. If it is only required for a set period of time, planning must also be in place for secure destruction of the personal information.
PART 1 – CONSIDERATION OF PERSONAL INFORMATION PRIVACY

(APP 1) Open and Transparent Management of Personal Information

The Institute is committed to managing personal information in an open and transparent manner and in accordance with the APPs. To achieve this, the Institute will ensure it has an up-to-date Privacy Policy and will make this Policy available on request and free of charge in an appropriate form. If a person requests a copy of the Institute’s Privacy Policy in a particular form, the Institute will take reasonable steps to provide the Policy in that requested form.

The Institute also makes available via its website, free of charge, a Privacy Statement that outlines in short form, the Institute’s approach to privacy matters.

Complaints in relation to the Institute’s handling of personal information can also be directed to the Privacy Officer, whose details are listed on Page 2 of this document.

(APP 2) Anonymity and Pseudonymity

Where it is lawful and practicable to do so, the Institute will allow individuals to provide information anonymously or using a pseudonym.

An individual who chooses to access the services of the Institute anonymously or using pseudonym will be notified of any potential consequences resulting from their decision.

The Institute will not prevent an individual from participating in the Institute’s activities because they request anonymity or uses a pseudonym.

PART 2 – COLLECTION OF PERSONAL INFORMATION

(APP 3) Collection of Solicited Personal Information

The Institute will only collect personal information reasonably necessary to undertake its programs, activities or functions.

- Personal information will only be collected by lawful and fair means and directly from the individual wherever possible.
- The name and contact details of the Institute will be supplied to the individual at or before the time of collection, or as soon as practicable after collection by the Institute.
- The Institute will ensure that each individual providing personal information is notified about the purpose of collecting the information, to whom or under what circumstances their personal information may be disclosed to another party, and how they can access the information held about them by the Institute.
- The Institute will ensure that individuals who are asked to provide personal information are notified about the consequences, if any, of not providing that information or of providing incomplete or inaccurate information.

Implementation

The Institute collects personal information for a range of reasons, which may include:
1. To communicate with the individual;
2. To operate and improve the Institute’s services;
3. For billing and other administrative purposes;
4. For educational and training, social enterprise and public health advocacy purposes;
5. For direct marketing with the purpose of encouraging financial support of the Institute; and
6. For research into the prevalence to eye disease in the community.

All information collected will be utilised in aggregated and de-identified format only.

Sensitive Information

Sensitive information is personal information concerning information or opinions about certain attributes of an individual (e.g. race or ethnicity, religion, political views or association, sexual orientation or practices, criminal history, health information etc.). The Institute will only collect sensitive information other than health information about an individual if:
- The individual consents and the information is reasonably necessary for one or more of the Institute’s functions or activities; or
- The collection is required by law, or a court or tribunal order; or
- A permitted general situation or a permitted health situation exists

As a non-profit organisation, the Institute may also collect sensitive information if the information relates:
- to the activities of the Institute; and
- solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities.

Implementation

The Institute will only collect and record sensitive information about people with their permission.

Whenever the Institute collects health related information from people, it will ask for permission to do so at the time of the collection and record that such permission was given.

The Institute will take reasonable steps to permanently de-identify the information before the organisation discloses it.

Any information recorded as sensitive collected by the Institute will be stored in a secure, locked location, with access restricted to those staff members required to access that information only. Electronic data will be encrypted and password protected.

(APP 4) Dealing with Unsolicited Personal Information

APP 4 is a new principle applying to the receipt of personal information which is not solicited. Unsolicited personal information must be afforded the same privacy protection as solicited personal information.

Where unsolicited personal information is received:
- an organisation must determine whether it could have collected the information under APP 3 (APP 4.1)
- if the information could have been collected, then APPs 5 to 13 apply to the information (APP 4.4)

From time to time an individual may voluntarily and without prompting by the Institute disclose to the Institute personal information about that, or any other individual (e.g. an employment application for an unadvertised position). Where the Institute receives such unsolicited personal information, the Institute will determine within a reasonable period whether it could have collected that personal information under APP
3 (e.g. whether the unsolicited information is reasonably necessary for one or more of its functions or activities).

If the Institute determines that it could not collect that personal information in accordance with APP 3, then as soon as practicable and where it is lawful and reasonable to do so, the Institute will either destroy the unsolicited personal information it receives, or permanently de-identify that unsolicited personal information. The Institute will otherwise treat any unsolicited personal information it receives as if it had solicited the collection of that personal information.

**(APP 5) Notification of the Collection of Personal Information**

Before, during, or as soon as practicable after the collection process, the Institute will notify individuals from which it has collected personal information about certain matters, including (amongst other matters) why their personal information is being collected, how it will be used and how to contact the Institute regarding their personal information. Where required by the APPs, the Institute will also obtain a signed informed consent from the individual. This is the responsibility of the staff member collecting the information and should be discussed with the Privacy Officer if there are any concerns or questions.

Staff collecting and recording personal information from the public should use the Privacy Checklist (Appendix A) to assist in considering the relevant issues and implementing the Privacy principles.

**PART 3 – DEALING WITH PERSONAL INFORMATION**

**(APP 6) Use or Disclosure of Personal Information**

The Institute will ensure that personal information will only be used for the purpose it was collected, or that would reasonably be expected by the individual providing the information.

If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, the Institute will obtain informed consent from the individual for that secondary purpose. Individuals will be given the opportunity to refuse such disclosure or use. If an individual is physically or legally incapable of providing consent, a responsible person (as described under the Act) may do so.

The Institute will usually not disclose personal information to other organisations. The Institute will only disclose personal information without consent where such disclosure is required by Australian law and court/tribunal order, or for law enforcement, or in the interest of the individual’s or the public’s health and safety. The Institute will keep records of any such use and disclosure. Information may be disclosed to a responsible person (as described under the Act).

**Disclosure to Contractors**

In circumstances where the Institute has contracted other organisations to carry processes to assist in direct marketing, e.g. mailhouse or database maintenance work on behalf of the Institute, special attention will be paid to privacy and confidentiality issues.

All such contractors must agree in writing to be bound by the Privacy Act regardless of whether they are legally bound by the Act. This agreement must be included in all future contracts entered into by the Institute and will include a clause about confidentiality of personal information provided by the Institute to the contractor.

**Other Legal Reasons for Disclosure**
- There may be other special circumstances that require the Institute to disclose personal information to external organisations. These are specified within APP2 under the headings of:
  - serious threats to life, health or safety
  - unlawful activity
  - required or authorised by law
  - enforcement bodies

  In these circumstances, the Institute will abide by APP6 in consultation with relevant government agencies and legal advisers before such a decision to disclose is made. Given the nature of the Institute and the information it holds, it is unlikely that such circumstances will occur frequently.

**(APP 7) Direct Marketing**

**Use of Information Collected Directly from Individuals**

The Institute may collect information in a number of ways (e.g. in person, over the phone, in writing direct from the person, by email etc.) that it uses for direct marketing purposes. Collection for direct marketing purposes only occurs where:

- The individual has not chosen to OPT OUT of direct marketing communications from the Institute or requested to do so. Any person opting out is recorded as soon as practicable in the Institute’s database to ensure that no further direct marketing materials from the Institute are sent to them.
- The individual has consented to the use or disclosure of sensitive information for direct marketing purposes if the information collected is sensitive information.

**Use of Information Collected from other Organisations**

If the Institute collects personal information from other organisations, eg; National Life Church Survey (NCLS), for the purpose of direct marketing. In such cases, the Institute will ensure that the organisation providing the information confirms in writing that all information provided by that organisation to the Institute was collected in accordance with the Privacy Act (including all necessary consents)

**Disclosure of Information to Others**

The Institute does not disclose personal information to any other organisations for direct marketing purposes.

**(APP 8) Cross-Border Disclosure of Personal Information**

APP8 prevents the Institute from disclosing personal information to someone in a foreign country (other than to the individual that the personal information is about) without first taking reasonable steps in the circumstances to ensure that the recipient does not breach the APPs in relation to the disclosed information.

This means that the Institute will only transfer personal information about an individual to someone who is in a foreign country if:

- The individual consents to the transfer after being informed that such consent will excuse the Institute from taking reasonable steps to ensure that the recipient does not breach the APPs in relation to the disclosed information; or
- The Institute reasonably believes that the recipient is bound by law or a binding scheme that has the effect of protecting the disclosed information that is at least substantially similar to the way the APPs protect the information, and the individual can access and take action to enforce that protection; or
- The disclosure is required by law or a permitted general situation exists in relation to the disclosure by the Institute; or
- The data is de-identified

(APP 9) Adoption, Use or Disclosure of Government Related Identifiers

Generally speaking, the Institute must not adopt, use or disclose an identifier that has been assigned by a Commonwealth or State/Territory agency to identify personal information.

Implementation

The Institute donor database has a system of allocated donor numbers, which identifies each individual record with a unique number not related to any information provided by the individual or related to any other system.

The Institute will not use Commonwealth Government agency identifiers as part of its personal records. This includes not using Tax File Numbers or Medicare Numbers.

The Institute may receive information from the HIC for the reimbursement of Eyecare services to patients. This payment (reimbursement) utilizes provider numbers of the individuals providing the service, and the names and Medicare numbers of the patients receiving the service. The Institute will maintain this data in a locked, secured location once quality assurance checking has been completed by the service provider.

PART 4 – INTEGRITY OF PERSONAL INFORMATION

(APP 10) Quality of Personal Information

The Institute will take reasonable steps to ensure that personal information kept, used or disclosed by the Institute is accurate, complete, relevant, not misleading and as up-to-date as practicable.

Implementation

The Institute will maintain all information records to be as up-to-date as possible. This happens most often when the Institute receives direct marketing material returned by Australia Post and from corrections noted on direct marketing materials by people themselves.

In each case, the Institute will process the changes and update the database record of personal information as soon as possible so that mail is not sent to the incorrect address.

Individuals can otherwise contact the Institute at any time to have any personal information held by the Institute about them corrected. Where an individual requests the Institute to correct any personal information, the Institute will take reasonable steps where permitted by law to correct that information, and where requested by the individual, will also request any third parties to which that personal information has been disclosed to do the same.

(APP 11) Security of Personal Information

The Institute must take reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access modification or disclosure.

Implementation
All personal information held by the Institute will be, if in paper form, received and stored in a secure, locked location.

The Institute will destroy or permanently de-identify personal information that is no longer required (as per existing legislation and research policy).

All staff of the Institute will maintain a Clean Desk Policy where all files relating to personal information are returned to the appropriate locked area at the close of business and where personal information is not left displayed on computer monitors when a work station is unattended.

If in electronic form, the Institute will ensure that all personal information transmitted electronically will be appropriately encrypted before transmission.

Only authorised staff will have access to personal information stored by the Institute and that personal information will not be discussed or provided to unauthorised staff and will not be taken from the Institute’s premises unless authorised and for a specific reason.

Staff should maintain the confidentiality of their computer passwords.

All staff, volunteers, contractors and board members will be required to sign an Institute confidentiality agreement requiring them to keep all personal information that they have access to completely confidential.

In regards to the Ethics of research, information collected this needs to be stored in a locked cupboard for seven (7) years.

The Institute Offices are based on Level 4, Rupert Myers Building, University of New South Wales. Access to Level 4 has security card access only – no general public access without staff member present. Internal doors between floors are also fitted with security card access only.

Non-compliance & Disciplinary Actions

Any Institute employee or relevant third party that identifies, knows about or suspects a Privacy breach must immediately report the matter to the Privacy Officer.

Employees or other relevant parties that contravene or do not comply with the Institute’s Privacy Policies and Procedures may be subject to disciplinary action.

Contractual Arrangements

The Institute will ensure that all contractual arrangements with third parties adequately address privacy issues.

Privacy Audits

The Institute will conduct periodic privacy audits in order to ascertain:

- what sort of personal/sensitive information is collected and held;
- how that information is collected;
- what the reasons are for collection of that information;
- where and how that information is stored;
- how that information is secured;
- who has access to that information;
- whether that information is shared with any one;
- whether the intended use of collection is communicated; and
PART 5 – ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION

(APP 12) Access to Personal Information

The Institute may give an individual access to personal information it holds about that individual on request.

Implementation

The Institute will deal promptly and courteously with all requests for access to information about personal records and will correct information shown to be incorrect and will respond to the person.

- All requests for access to personal information should be directed immediately to the Privacy Officer.
- The Institute will not charge for access to personal information
- People will be asked to put in writing their requests for access to a copy of personal information kept about them. The Institute will seek to check their identity by matching records and known information
- A written response to the request will be provided within 14 days if the request is straightforward or 30 days if it is more complicated
- The Institute will provide a written copy of information reasonably requested by the person
- There are few situations that would cause the Institute to refuse a request for access to a person’s personal information held by the Institute and these would only occur given the clauses contained in APP 12.2 or 12.3. (See Australian Privacy Principles reference material.) If the Institute refuses to give access to the personal information because of 12.2 or 12.3 the Institute will provide a written notice that sets out the reasons for refusal and mechanisms available to complain about refusal and any other matter prescribed by the regulations. If the Institute refuses to give access because of 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

(APP 13) Correction of Personal Information

An individual may request the Institute to correct personal information it holds about the individual. Such requests will be dealt with within a reasonable period from receipt of that request. If a person is provided with a copy of their personal information and can show that the record is incorrect, the Institute will correct the information as soon as practical and note the correction on the record. If the individual requests that other entities to which the Institute has disclosed that personal information to be informed of the correction, the Institute will also take reasonable steps to notify that other entity of the corrections. If a person disagrees with the Institute about the accuracy, completeness, relevance, currency, or misleading nature of the information held by the Institute, a note will be recorded that there is a difference of opinion about that information. If the Institute does not correct the information, the individual may request that a note be associated with the uncorrected information regarding the information’s inaccurate, incomplete, irrelevant, or misleading nature. The Institute will take reasonable steps to comply with such a request to make the note apparent to other users of the information.
APPENDIX A

Privacy Checklist

All Institute staff planning a program which involves the collection of people’s personal information should consider the following list of questions and issues and refer to the Institute Privacy Policy and Privacy Officer if they have further questions.

- Clearly identify why you are collecting people’s personal information. Be sure that collecting the information is necessary

- Determine what information you will collect. Check if any of it is health related and may be considered sensitive under the Privacy Act

- Identify how you will collect the information

- Identify what the information will be used for

- Identify the use of the information, as to whether the Institute will want to use that information for other purposes, e.g.; direct marketing of appeal materials

- When you collect the information from people, include details on what the information will be used for and how they can contact the Institute if they have any questions. Have this process approved by the Institute Privacy Policy Officer prior to implementation.

- Identify, whilst meeting the APPs, how and where the information will be kept and ensure that it is secure and only accessible by authorised people.

- Identify how long the information will be kept as per current legislation and how the data will be stored and accessed once the project finishes. If the data is no longer required, and there exists no legislative requirement to store the data, decide how it will be destroyed.
APPENDIX B

Privacy Statement

At the Brien Holden Vision Institute ABN 49 081 303 282 (the ‘Institute’) and the Brien Holden Vision Institute Foundation ABN 86 081 872 586 (the ‘Foundation’) we take seriously your privacy and our obligations under the Privacy Act 1988 (Cth) as amended from time to time (the ‘Privacy Act’). Each reference in this Privacy Statement to ‘we’, ‘us’, and/or ‘our’ is a reference to both the Institute and the Foundation. References to the ‘website’ means the www.brienholdenvision.org website.

This Privacy Statement is a summary of our Privacy Policy and aims to inform you about our collection, use, disclosure and storage of your personal information. Further information about our general privacy practices can be found in our full Privacy Policy, which is available on request through our Privacy Officer.

This Privacy Statement and our Privacy Policy are effective as at 1 September 2016. We may need to update or change them from time to time so it is recommended that you review them at any time you are proposing to supply personal information to us. We will post an updated version of our Privacy Statement on our website if this happens.

By using this website or supplying us with your personal information, you agree to the terms of this Privacy Statement and our Privacy Policy.

What information is being collected?

From time to time we may collect personal information as defined under the Privacy Act through one of a number of interactions that you might typically conduct with us.

We may collect personal information from you in a number of ways, including directly from you when you provide this information to us by phone, in person, by email or when you submit personal details through our online forms or registration on the website.

The type of personal information we collect from you will depend on how you interact with us, but typically includes name, address, e-mail address, fax and telephone numbers, and payment information (for example, if you’re donating to the Institute or Foundation). Sometimes, we may also collect health information or other sensitive information about you. On such occasions we will seek your consent to the collection and use of that information.

There may be times when we ask you for personal information and you may not wish to provide it. You are not obliged to provide such information, but it may result in us being unable to provide you with a particular service that you want.

From time to time we may ask you to complete surveys for research purposes and may keep a copy of your responses. You are not obliged to respond to such surveys.

Sometimes we may also receive personal information about you without asking for it. Where we receive such unsolicited personal information, we will treat that information in accordance with the Australian Privacy Principles and destroy or permanently de-identify any personal information within a reasonable amount of time if we determine that we could not have collected that information in accordance with the Australian Privacy Principles. Normally, this means we would have to be able to collect the personal information using fair and reasonable means and for a particular purpose reasonably necessary for, or directly related to, one or more of our functions or activities.

Specific to the website, we may perform statistical analysis of subscriber and user activities and characteristics. For this, we may collect non-personal information, including information about your computer and browsing preferences, through the standard operation of our servers or through the use of cookies. This type of information does not identify any individual but is statistical data about our users’ browsing activities and patterns. The information we may collect for this may include:

- Your server address;
• Your top level domain name (for example .com, .gov, .au, .uk etc);
• The date and time of your visit to the site;
• The pages you accessed and the document downloaded;
• The previous site you visited; and
• The type of browser you are using.
If you do not want information collected through the use of cookies, you should use your browser’s cookie disabling feature. If cookies are disabled, however, certain features may not be available to you. The use of cookies allows us to enhance the functionality of the service we offer to users of the website.

How is personal information used?

We collect personal information for a range of purposes, including to communicate with you, for subscriber and user identification, providing services, operating and improving our sites, billing and related administration. We may share the information you have given to us with our other companies within the group, our associates and affiliates.

We may also use your personal information for related purposes that you would reasonably expect such as:

• Providing you with information and services that you may request;
• Providing you with updates and new service announcements;
• Allowing you to participate in interactive features of the website should you choose to;
• Carrying out our obligations in any contracts with you.

Direct marketing

There may be circumstances where we may collect, collate and use any personally identifiable information and any other information you submit to us for the purpose of sending to you, either through us or through our associates or affiliates, marketing and promotional messages and communications campaigns. If we use your personal information for direct marketing purposes, we will give you the opportunity to opt out of receiving any further marketing material.

At times we may contract out a service to a third party and we may need to disclose your personal information to that third party so you receive the services needed. We will not permit any third parties to which we have disclosed personal information to use such information for any purpose save for the purpose for which it was disclosed in accordance with our Privacy Policy.

How we hold personal information

Personal information collected from you may be held and stored in hard copy or electronic format and processed in Australia or in any other country in which we or our affiliates, subsidiaries or our service providers maintain facilities. This may include but is not limited to Australia, Cambodia, Vietnam, Pakistan, Sri Lanka, Papua New Guinea, Fiji, China, Colombia, Haiti, South Africa, Mozambique, Malawi, Eritrea, Kenya, Nigeria, Mali, Uganda, Ethiopia, Tanzania, India. In such cases, we will strive to comply with all relevant applicable laws that are designed to protect your privacy. Although legal requirements may vary from country to country, we will take reasonable steps to ensure that the information which we have transferred will be held, used or disclosed by the recipient of the information consistently with the Australian Privacy Principles under the Privacy Act.

When we disclose your personal information

We may disclose your personal information to third parties where required to do so by law, or where necessary to lessen or prevent a serious threat to the life, health or safety of others or the public.

Security of personal information

We take reasonable steps to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. We also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.

To this end, we take reasonable steps to provide a secure environment and have internal security measures in place to deal with the physical security of our premises and the personal information kept at our premises. We also have procedures in place designed to maintain a secure computer and electronic system and to make our staff aware of their obligations when dealing with personal information.
You should be aware that there are inherent risks associated with the transmission of information via the internet, and we cannot guarantee the safe and secure transmission of information to or from us unless we explicitly say so in writing for a particular interaction.

Third party sites
Any links on the website to other sites are provided for convenience only. We assume no responsibility or liability for the information collection and disclosure practices of any sites that a user may access through the website. We are not responsible for the content and privacy policies of other sites, and recommend that you review each site’s privacy policy.

Your rights to access and correct your personal information
You can request access to your personal information (if any) that we keep on record and we will provide you with access to such personal information. Please contact our Privacy Officer by the means set out below if you would like to make such a request.

We take reasonable steps to make sure that the personal information we collect, use or disclose is accurate, complete, up-to-date, relevant and not misleading. If you believe any information that we keep on record is inaccurate, incomplete, out-of-date, irrelevant, or misleading, you may request that it be corrected. There is no fee for requesting access to your personal information; however, we may charge you the reasonable administrative costs of processing your request.

We encourage you to advise when personal information you have supplied to us is no longer valid or needs updating.

Complaints
If you are concerned that there may have been some inappropriate use or disclosure or any other breach relating to the use of your personal information, we want to hear about it. All complaints we receive will be investigated under our Privacy Complaints Policy. If you have any such complaints please contact our Privacy Officer.

Privacy Complaints Policy - Introduction
This document outlines the procedures we use for dealing with privacy complaints.

We will refer all complainants with complaints or disputes about the collection, use, disclosure and protection of their personal information or other privacy issues to our Privacy Officer (contact information below).

At all times this policy will be governed by the following principles:

- All complaints will be treated seriously
- All complaints will be dealt with promptly
- All complaints will be dealt with in a confidential manner.

What is a privacy complaint?
A privacy complaint relates to any concern that you may have regarding our privacy practices or our handling of your personal information. This could include matters such as:

- How your personal information is collected or stored;
- How your personal information is used or disclosed; and
- How access is provided to your personal information.

Who may make a complaint?
If you have provided us with personal information or we have collected and hold your personal information, you may make a complaint, have it investigated and dealt with under this policy.

How to make a complaint?
You may contact our Privacy Officer by phone, by post or through the webform available on our website [link here]. Contact details are:

The Privacy Officer
Complaints should specify the nature and substance of the complaint and the relevant date. You will need to provide as much information as possible to assist us in our investigation. All complaints will be logged on our database.

**Complaints resolution procedure**

Once the complaint has been made, we will try to resolve the matter in a timely fashion as follows:

- You should receive acknowledgement of receipt of your complaint within 14 days of the date you lodge it.
- We may request further information from you. This will enable us to investigate the complaint and determine an appropriate solution. All details provided will be kept confidential.
- It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to progress your complaint.
- If your complaint involves the conduct of our employees we will raise the matter with the employee concerned and seek their comment and input in the resolution of the complaint.
- If your complaint is not able to be resolved at a local level it will be referred to our legal advisers. You will be notified if this happens.
- You will be informed of the outcome of the investigation, the action taken to resolve the issue and the changes made to prevent this matter recurring.
- If the Privacy Officer determines, either before or after an investigation, that the complaint is not well-founded, the Privacy Officer will inform the complainant in writing of this decision and the reasons for it.
- If the complaint is not resolved to your satisfaction, you are entitled to refer your complaint to the Office of the Australian Information Commissioner (www.oaic.gov.au).
- We will keep a record of your complaint and the outcome.

**Further Information**

For further information about this Privacy Statement or to obtain a copy of our full Privacy Policy please contact our Privacy Officer.