PRIVACY POLICY

This privacy policy provides information on how Capitol Strata Management Pty Ltd trading as Capitol Body Corporate Administration and Delrey Pacific Pty Ltd trading as Capitol Body Corporate Administration Redcliffe (collectively referred to as Capitol) manage personal information collected by Capitol.

Capitol is bound by the *Privacy Act 1988* (Cth) (Act) and the Australian Privacy Principles (APPs) set out in the Act. This Privacy policy will apply to all dealings with us, whether in person, or via telephone, email, correspondence or our website at www.capitolbca.com.au.

Capitol will ensure that all officers, employees and subcontractors are aware of and understand Capitol's obligations as well as their own obligations under the Act. We will achieve this through the provision of training and through maintaining and implementing internal policies and procedures to prevent personal information from being collected, used, disclosed, retained, accessed or disposed of improperly.

What is 'personal information'?
'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.

Collection of personal information
Capitol collects personal information in order to carry on its business as a Body Corporate Manager and provider of administration and secretarial services for Community Title Schemes and other communities of people, all collectively called body corporate management services.

The information which we collect will depend upon the reason for which it is collected. The main reasons are:

- To provide Body Corporate Management Services - in the course of managing a Community Titles Scheme or other community we are likely to collect personal information about individual Owners and third parties. The type of personal information collected may vary from Owner to Owner; but will in the main be limited to:
  - Full name;
  - Address/es including residential address, business address and postal address;
  - Other contact details including telephone numbers and email address
- For marketing - during meetings and in the course of communications with individual Owners and contacts we sometimes collect their contact details in order to be able to send them newsletters and updates about legal developments and other matters of interest relating to body corporate legislation and community living or to otherwise market our services to them;
- To respond to comments, enquiries or requests made via our website.

Capitol does not collect sensitive information regarding individuals. Sensitive information includes but is not limited to information about an individual's:

- racial or ethnic origin;
- religious beliefs or affiliations;
- membership of a trade union;
- sexual orientation or practices;
- criminal record;
- medical records.

If we receive sensitive information that we did not solicit, then we will (if it is lawful and reasonable) destroy the information.

Capitol will, if it is reasonable or practicable to do so, collect personal information directly from the relevant individual.

Sometimes we will collect personal information from a third party or a publicly available source. For example, we may need to collect personal information from an individual's legal adviser, from an individual's past or current real estate agent or letting agent, from a resident unit manager or caretaker of a body corporate scheme in which the individual resides from an individual's financial institution, etc.

If we receive personal information that we did not solicit, we will determine as soon as reasonably practicable whether we could have lawfully collected that information as part of our functions or activities. If we are not satisfied that we could have lawfully collected the information, then we will (if it is lawful and reasonable) destroy the information or ensure that it is de-identified.

Individuals may choose to deal with Capitol anonymously or under a pseudonym where lawful and practical. Where anonymity or use of a pseudonym will render us unable to provide the relevant service or do business, we may request that an individual identify him or herself. For example, whenever documents are to be submitted to a court, or a government agency, it may be necessary that we record an individual's name accurately.

Use and disclosure of personal information
Any personal information collected by Capitol will only be used and disclosed for the purpose for which it has been provided to us or as authorised under law.

We may use your contact details to send you firm newsletters, legal or other updates relating to community living or invitations to Capitol seminars or events, which may be of interest to you. However, you may at any time opt out of receiving such materials by contacting Capitol on team@capitolbca.com.au or sending a request to the address below. Upon receiving such a request, Capitol will remove your contact details from our distribution lists.

Capitol may transfer your personal information to overseas countries including but not limited to the Philippines, the United States of America or European Union countries in order to perform one or more of our functions or activities. In these circumstances, we will take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the information.

Personal information may need to be disclosed to external service providers or third parties engaged by Capitol in order for those service providers to fulfil their service obligations to the firm.

For example:

- IT service providers who assist in managing Capitol's servers and networks may need to access client data in order to maintain the servers and networks;
- Outsourcing contractors and individuals who are resident in the Philippines who carry out certain tasks and do work for Capitol to assist in the performance of one or more of our functions or activities.

Where personal information is disclosed to an external party, Capitol will take reasonable steps to ensure that the external party treats such information confidentially and in accordance with the APPs.

There may be circumstances in which it is necessary for Capitol to collect an individual's government related identifier such as a tax file number or Centrelink reference number. We will not use or disclose government related identifiers unless we are required or authorised to do so by law or by a Court or Tribunal order, or in order to fulfil our obligations to a State or Territory authority.

Accuracy of Personal Information
Capitol will take reasonable steps to ensure that all personal information it collects, uses or discloses is accurate, complete and up-to-date.

If you believe your personal information is not accurate, complete or up-to-date, please contact us (see the **Contacting Us** section for more information).

Security
Personal information may be stored by Capitol in hard copy documents or electronically. Capitol is committed to keeping personal information secure and safe. Some of the ways we do this are:

- Requiring employees and contractors to enter into confidentiality agreements.
- Security measures for access to our computer systems.
- Providing a discreet environment for confidential discussions.
- Access control for our buildings.
- Security measures for our websites (see the **Your Privacy on the Internet** section for more information).

We will review and update our security measures from time to time.

In addition, we will review the personal information held by us from time to time, ensuring that information which is no longer needed for a purpose for which it was initially collected is destroyed or de-identified (provided it is lawful for us to do so).

PRIVACY POLICY

Your Privacy on the Internet
Capitol takes care to ensure that the information you provide to us via our website is protected. For example, our website has electronic security systems in place, including the use of firewalls.

You may be able to access external websites by clicking on links we have provided. Those other websites are not subject to our privacy standards, policies and procedures. You will need to contact or review those websites directly to ascertain their privacy standards, policies and procedures.

Capitol's internet service provider makes a record of each visit to Capitol's website. When you visit our website, the following information is logged for statistical purposes only:

- your server address;
- your top level domain name (for example .com, .gov, .au, etc);
- the date and time of your visit to the site;
- the pages accessed and documents downloaded by you;
- the previous site visited by you;
- the type of browser used by you.

When you visit our website, our server will attach a small data file called a "cookie" to your computer's memory (unless your web browser is set to refuse cookies).

A "cookie" is a very small text file placed on your hard drive for record keeping purposes by our web page server. The cookie's purpose is to notify our web page server that the same visitor has returned to our website and to collate anonymous information on when and how our website is used.

The information collected is not linked to your identity in any way or any other information provided by you.

Email Communications
If you have registered through our website to receive email communications from us and later change your mind, you may contact us to have your name removed from our distribution lists.

Accessing and Correcting Personal Information
You may request access to personal information that Capitol holds about you (see the **Contacting Us** section for more information).

We will acknowledge your request within 5 business days of the request being made. If access is being denied, we will usually advise you in writing of the denial of access and the reasons for same within 10 business days of our acknowledgement. If access is being granted, access will usually be granted within 10 business days of our acknowledgment or, if the request involves complex considerations or voluminous photocopying or scanning, within 10 business days. We will let you know which timeframe applies to your request and if any delays are anticipated.

You will need to verify your identity before access to your personal information is granted.

While we cannot and do not charge an '*application fee'* for you applying to access your personal information, we may charge a fee for actually giving you access to your personal information in your preferred format (where reasonable and possible), which will cover our costs involved in locating and collating information as well as reproduction costs.

Once your request has been processed by us, you may be forwarded the information by mail or email or you may personally inspect it at the location where the information is held or another appropriate place. Whenever possible, we will endeavour to make the information available to you in the manner requested by you unless it is unreasonable for us to do so (e.g. if you have asked for the information to be emailed to you, we will endeavour to email the information to you. If the file size would be too large, we may send you the information by hard copy instead of email).

If you are aware that we hold personal information about you that is no longer accurate, complete or up-to-date, please contact us (see the **Contacting Us** section for more information).

If you request access to your personal information, or if you request that we correct your personal information, we will allow access or make the correction unless we consider that there is a sound reason to withhold the information, or not make the correction.

Under the Act, we may refuse to grant access to personal information if:

- We believe that granting access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.
- Granting access would have an unreasonable impact upon the privacy of other individuals.
- Denial of access is required or authorised by law or by a Court or Tribunal order.
- Giving access would be unlawful.
- The request for access is frivolous or vexatious.
- Legal proceedings are underway or anticipated and the information would not be accessible by way of the discovery process in those proceedings.
- Giving access would reveal our intentions in relation to negotiations between us and you in such a way as to prejudice those negotiations.
- Giving access is likely to prejudice enforcement related activities conducted by, or on behalf of, an enforcement body.
- Giving access is likely to prejudice action being taken or to be taken with respect to suspected unlawful activity or serious misconduct relating to our functions or activities.
- Giving access would reveal information in connection with a commercially sensitive decision making process.

If we do not agree to make a correction to your personal information, you may provide a statement about the requested corrections and we will ensure that the statement is apparent to any users of the relevant personal information.

If we do not agree to provide access to your personal information or to correct your personal information, we will provide written reasons for the refusal and the mechanisms available to complain about the refusal (see the **Complaints** section for more information).

Complaints
It you believe there has been a breach of the APPs, you are entitled to complain to us. Please direct any complaints to our privacy contact (see the CONTACT US section for more information). We will investigate your complaint and endeavour to resolve it.

If you consider that we have not dealt with your complaint adequately, you may complain to the Office of the Australian Information Commissioner on the below details:

Post:
Office of the Australian Information Commissioner (OAIC)
GPO Box 5218
SYDNEY NSW 2001

Email: enquiries@oaic.gov.au
Telephone: 1300 363 992

Contacting Us
To contact us about any privacy matter or to notify us that you wish to be removed from our distribution lists, please either:

- send us an email to: team@capitolbca.com.au; or

- send us a letter addressed as follows:
  The Privacy Officer
  Capitol Body Corporate Administration
  PO Box 2362
  CHERMSIDE CENTRE QLD 4032

Changes to Capitol's privacy policy
This privacy policy is effective from 1 May 2014. From time to time it may be necessary for us to revise our privacy policy. Capitol reserves the right to change our privacy policy at any time without prior notice. We will notify you of the changes by posting an updated version of the policy on our website at www.capitolbca.com.au.

PRIVACY POLICY

AUSTRALIAN PRIVACY PRINCIPLES

From 12 March 2014, the Australian Privacy Principles (APPs) replaced the National Privacy Principles and Information Privacy Principles and apply to organisations and Australian Government agencies. This fact sheet provides a summary of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which amends the *Privacy Act 1988*. For the latest versions of these Acts visit the ComLaw website: www.comlaw.gov.au.

Australian Privacy Principle 1—open and transparent management of personal information

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

Australian Privacy Principle 2—anonymity and pseudonymity

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

Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

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

Sensitive information

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

(a) If the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities;

Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) An APP entity receives personal information; and

(b) The entity did not solicit the information;

The entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information and, if not, the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

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

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) To notify the individual of matters regarding the collection of such information as are reasonable in the circumstances; or

(b) To otherwise ensure that the individual is aware of any such matters.

Australian Privacy Principle 6—use or disclosure of personal information

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

Australian Privacy Principle 7—direct marketing

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

Australian Privacy Principle 8—cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) Who is not in Australia or an external Territory; and

(b) Who is not the entity or the individual;

The entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

9.1 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.

Australian Privacy Principle 10—quality of personal information

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

Australian Privacy Principle 11—security of personal information

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

Australian Privacy Principle 12—access to personal information

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

Australian Privacy Principle 13—correction of personal information

13.1 If:

(a) An APP entity holds personal information about an individual; and

(b) Either:

(i) The entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) The individual requests the entity to correct the information;

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