

COASTLINE CREDIT UNION LTD
PRIVACY POLICY

Coastline Credit Union Ltd recognises the importance of your privacy, and is committed to protecting personal information about you that we hold. This Privacy Policy describes how we manage personal information and safeguard privacy.

Any reference to 'us', 'we', 'the Credit Union' or 'Coastline Credit Union' in this document is a reference to Coastline Credit Union Ltd

1. NATIONAL PRIVACY PRINCIPLES

From 21 December 2001, most private sector organisations in Australia must by law comply with the National Privacy Principles ("NPPs"). The NPPs strengthen protection of your privacy. We will comply with the NPPs from that date.

2. COLLECTING PERSONAL INFORMATION ABOUT YOU

The Credit Union holds only those kinds of personal information that are necessary for us to perform our functions. This in turn depends upon the type of product or service you request from us. It may include:

- 2.1 Information you give us when you apply for or request a product or service from us. The information will include your name, address and contact details. If you fail to give us the information we ask for, we may be unable to process your request for a product or service.
- 2.2 Financial information about you, such as your financial position. We will only hold information obtained from credit checks if you have authorised us to carry out those checks.
- 2.3 Communications between you and us.
- 2.4 Transactional information about a product you have or have had with us.

We may also collect some information about you when you use our website www.coastline.com.au:

- When you visit the website, our server has the ability to attach a small data file, called a cookie, to your hard drive for our record keeping purposes. We do not store any information inside cookies. Cookies are a feature of most websites. Most web browsers are set to accept cookies, but may be set to refuse them. We may use cookies to provide us with aggregate and anonymous information on how people use the website and what they find interesting and useful on it. We do not link this information back to any information you have given us.
- As most websites do, we track usage patterns on an anonymous and aggregate basis. Your identity cannot reasonably be ascertained from this information. Each time you visit the website, a web server records your visit, and information that includes your internet provider's address, the date and time of your visit, the pages accessed and documents downloaded and any search items entered.
- If you visit the website to complete an online form such as online loan application or to send us an email we will record the information you give us, including your email address.

Thus, your use of the facilities and information available on the website will determine the type and amount of personal information we collect about you.

3. USING AND DISCLOSING YOUR PERSONAL INFORMATION

3.1 We respect your privacy. Any personal information which we collect about you will be used by us to:

- (a) Provide you with the products or services you have requested, or
- (b) Assess an application by you for products or services we may provide and if that application is approved, to provide them to you.

In addition, we may also use your personal information to provide you with information about other products and services offered or distributed by us or our related companies. However we will only do this with your consent. Where possible, we store any personal information about you anonymously. We do not use external identifiers to assist us in the management of personal information.

3.2 We store your personal information with a strong emphasis on its security and the protection of your privacy. In considering the security of your personal information, we have taken into account:

- (a) Physical security:
 - (i) All files containing personal information are secured in locked cabinets after hours and during business hours when not in use. The credit union requires its staff to maintain a clean desk policy.
 - (ii) All files containing personal information are accessible only by staff requiring them for the completion of specific duties.
 - (iii) All hard copies of identification items such as passports and drivers licences are destroyed by means of a secure destruction service after the entry onto the database of the information they contain.
 - (iv) Drafts, spare copies and extra materials generated in the handling of files containing personal materials are destroyed by means of a secure destruction service.
 - (v) Personal information that is no longer required is permanently de-identified or destroyed by means of a secure destruction service.
 - (vi) Information about closed accounts is held for seven years at a secure off site facility and at the end of the seven year period the information is destroyed by means of a secure destruction service.

- (b) Computer and network security:
 - (i) Access to the computer network is by user identification and password only. Passwords are changed regularly. The system administrator can identify all users by their user identification.
 - (ii) The system administrator regularly reviews computer logs for security breaches and reports any breaches to the relevant manager.
 - (iii) Computer files are regularly reviewed for continued relevance by a staff member with appropriate security clearance and where necessary deletion and purging of files no longer required is undertaken on a system wide basis.
 - (iv) Files are regularly backed up and saved at a separate and secure site.
 - (v) Network security includes firewall and virus protection and network intrusion detection systems.

- (c) Communications security:
 - (i) No personal information is provided at branches, over the telephone or by facsimile until the identity of the applicant is verified.
 - (ii) Access to telephone banking is password protected.
 - (iii) Security for Internet banking is provided by use of 128 bit encryption of data for transmission, secure socket layers protocol and password anonymity.

- (d) Personnel security:
 - (i) Hard file and computer copies of unsuccessful applications for employment are destroyed by means of a secure destruction service. Appropriate and lawful enquiries are made before an offer of employment is made to any person.
 - (ii) Access to your personal information is given to staff strictly on the basis of their need to have access to the material in order to fulfill their function within the credit union.

- 3.3 In order to provide our services to you and to provide you with information about other products and services offered or distributed by Coastline we may disclose your personal information to organisations to which we contract out functions.
- 3.4 We will not pass on member information to other organisations to join a mailing list for junk mail.
- 3.5 External services providers to whom we contract out some of our functions include: IT, mailing, statements, electronic payment processing, card processing, chequing, withdrawals and deposits, legal, auditing, collection and insurance.

4. ACCESS TO YOUR PERSONAL INFORMATION

- 4.1 From 21 December 2001, in most cases, you can gain access to personal information we hold about you. We will handle requests for access to your personal information in accordance with the NPPs. All requests for access to your personal information will be handled by our Member Services Manager, who can be contacted by telephone or in writing at the telephone number and postal and email addresses set out in item 5 below.
- 4.2 We will deal with all requests for access to personal information as quickly as possible. In any event, we will make an initial response to your request within 30 days. Requests for large amounts of information, or for information not currently in use, may require some time before a full response can be given.
- 4.3 In some circumstances under the NPPs we may refuse to give you access to personal information we hold about you. These are circumstances where giving you access would:
 - (a) Pose a serious and imminent threat to the life or health of any individual;
 - (b) Have an unreasonable effect upon the privacy of other individuals;
 - (c) Give you access to material which would not be accessible by the process of discovery in existing or anticipated legal proceedings between you and us;
 - (d) Reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
 - (e) Be unlawful;
 - (f) Be likely to prejudice an investigation of possible unlawful activity, or
 - (g) Be likely to prejudice:

- (i) The prevention, detection, investigation, prosecution or punishment of criminal offences, or certain other breaches of law;
- (ii) The enforcement of laws relating to the confiscation of the proceeds of crime;
- (iii) The protection of the public revenue;
- (iv) The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct, or
- (v) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
- (vi) By or on behalf of an enforcement body.

We may also refuse access if:

- We consider the request for access is frivolous or vexatious;
- We are required or authorised by or under law to do so, or
- An enforcement body performing a lawful security function asks us not to do so, on the basis that to do so would be likely to cause damage to the security of Australia.

If we refuse to give you access to the personal information you request, we will under the NPPs provide you with reasons for our refusal.

- 4.4 We wish to ensure that your personal information is accurate, complete and up to date. Generally, if you request us to do so, we will amend any personal information about you that is inaccurate, incomplete or out of date. If we disagree with you about any of these matters, and if you request us to do so, we will take reasonable steps to associate a statement to the effect that you claim the information to be inaccurate, incomplete or out of date with your personal information.
- 4.5 There will be no charge for lodging a request for access to personal information. However, we may charge you for providing access. Any charges will not be excessive. A schedule of current charges is available upon request at all branches and is published on our website.

5. CONTACTING US FOR FURTHER INFORMATION

You can get more information about the way we manage personal information about you which we hold by contacting us at the telephone number, postal or email addresses set out below.

If you are concerned that we may have breached your privacy and wish to make a complaint, please contact us at the telephone number, postal or email addresses set out below.

Contact details:

- For access to your personal information or to request a change to personal information held contact Member Services Manager, Telephone 02 65621066, Mail PO Box 3119 West Kempsey 2440, Email mail@coastline.com.au
- To receive further information about the way we manage personal information contact Member Services Manager, Telephone 02 65621066, Mail PO Box 3119 West Kempsey 2440, Email mail@coastline.com.au
- To complain about a breach of privacy contact Member Services Manager, Telephone 02 65621066, Mail PO Box 3119 West Kempsey 2440, Email mail@coastline.com.au

6. CHANGES TO OUR PRIVACY POLICY

From time to time it may be necessary for us to review and revise our privacy policy. We reserve the right to change our privacy policy at any time. If we do change this privacy policy we will post amended versions in all our branches and post an updated version on our website.

SCHEDULE OF REVIEW AND AMENDMENTS

Date	<u>Action</u>
13/12/2001	Adopted by Board of Directors.
18/11/2010	Board Review