



Share the difference

Privacy Policy

The obligations of this Policy:

1. Our Commitment

The protection of our members' privacy and maintaining confidentiality of our members' personal information is considered to be of the utmost importance and we take very seriously the ongoing trust that members place in us to protect their personal information.

In handling members' personal information, we are bound by and committed to complying with the Privacy Act 1988 (Commonwealth), the National Privacy Principles set out in the Act, applicable Codes of Practice and any other laws and codes regulating the collection, use, storage or disclosure of our members' personal information. We have a general duty to keep confidential all personal information we hold about our members, including members' names, addresses, financial data, and details of transactions on members' accounts.

Our Privacy Policy explains how we protect our members' privacy, including:

- how we collect personal information, and why we collect it;
- how we use personal information;
- the need for us to provide personal information to selected third parties to enable us to provide our members with the products and/or services that they request;
- the steps we take to protect and keep secure the personal information we hold; and
- how our members may access the personal information that we hold about them and the steps they may take if they believe that the personal information is not accurate.

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856
430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

2 Privacy Act

The national privacy scheme is a legislatively based framework of privacy laws for the Australian private sector. It is designed to give appropriate privacy protection to individuals when private sector organisations seek to collect, hold, use, disclose, correct or transfer their personal information.

The legislative framework for the Scheme comprises three tiers:

- New provisions in the *Privacy Act 1988 (Commonwealth)* introduced by the *Privacy Amendment (Private Sector) Act 2000*. These **have the force of law**.
- The National Privacy Principles contained in Schedule 3 of the *Privacy Act 1988 (Commonwealth)*. These **have the force of law**, however they are **worded in general terms**.
- The federal Privacy Commissioner has powers under section 27(1)(e) of the *Privacy Act 1988 (Commonwealth)* to make guidelines to help organisations avoid breaching the *Privacy Act 1988 (Commonwealth)*. Guidelines made under this power are **advisory and so are not directly legally binding**.

3 How we collect personal information, and why we collect it

We collect most personal information about our members directly from the members themselves. For example, we may collect personal information when a member opens a membership, completes an application form for one of our many products and services, deals with us over the phone, sends us a letter, visits our website, or has contact with us in person.

There may be occasions when we need to obtain personal information about one of our members from a third party – an example would be collecting personal information from a credit reporting agency if a member applies for a loan or credit facility.

Initially, we collect personal information from people to enable them to become members of our Credit Union. It is then used to enable us to provide them with the products and services that they apply for, or use.

We also collect it so that we can provide them with information about our products and services (marketing information), unless they tell us that they do not wish to receive it (refer section 7 below).

The personal information that we collect is only that which is necessary to enable us to provide our members with the products or services that they have requested. The types of personal information collected may include a member's:

- name and contact details;
- current residential address;
- current and past employers;
- annual income and other financial details; and
- date of birth.

In certain circumstances we may also need to collect sensitive information such as health details. For example, if a member decides to take out private health cover via our agency arrangement with Medibank Private, we may need to collect health information in our capacity as an agent.

4 We will use members' personal information for the primary purpose for which it was collected and for related secondary purposes

At or before the time we collect personal information we will advise our members of the primary purpose for which we will use it.

We will also give our members general advice as to related secondary purposes for which we may use the information, which may include:

- internal accounting and administration;
- regulatory reporting and compliance;
- servicing our relationship with each member; and
- protecting our members and us from error and fraud.

5 Providing personal information to third parties

Sometimes we may need to give some personal information about our members to other organisations who provide services that assist us in supplying, or in administering, the products and services our members require, or assist us in giving members the information that they are entitled to as members. Examples of such organisations are:

- our related entities (e.g. Eastwoods Wealth Management);
- Cuscal Ltd and its subsidiaries,
- Data Action Pty Ltd (our computer bureau);
- printing and mailing houses;
- insurers;
- valuers;
- legal advisors; and
- conveyancers.

These organisations may only use the information to the extent necessary to provide the services we require.

We may also exchange members' personal information with affiliated product and service providers and external product and service providers for whom we act as agent or referrer (so that they may provide members with the product or service they seek, or in which they have expressed interest, or which they may find of interest). Examples of such organisations are insurance companies, travel companies, credit card companies, and other financial services organisations.

Whilst we abide by our general duty of confidentiality, we may disclose our members' personal information if that disclosure is:

5.1 Required to comply with our legal obligations

This includes disclosure to various government departments and agencies (e.g. the Australian Taxation Office); disclosure to the Courts under subpoena; and disclosure to our auditors, APRA and AUSTRAC.

5.2 In the public interest

Where a crime, fraud, or misdeed is committed or is suspected, disclosure may be justified.

5.3 In our interest

This may include disclosure to a Court in the event of legal action to which we are a party; or necessary disclosure in connection with the sale of selected loans by us to a third party (securitisation).

We will not sell any personal information about our members to any other organisation.

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856

430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

6 Use of identifiers

We will not use our members' tax file numbers (TFNs), pension numbers, Medicare numbers or any other Commonwealth agency identifiers as identification records.

We will only use and disclose these numbers for the purposes required by law, such as disclosing members' TFNs to the Australian Taxation Office.

7 Consent for us to obtain and/or disclose personal information

We will only use a member's personal information for a purpose other than the primary purpose for which it was collected, or a related secondary purpose, with their consent.

In some circumstances a member's consent will be express. For example, when a member completes a loan application the member is invited to give the members' express consent for us to obtain a credit reference about the member from a credit reporting agency. Express consent is often given in writing, but it may be given orally.

In some circumstances a member's consent may be implied from the member's conduct. For example, a member may be invited to contact us if the member does not wish us to use personal information for a particular purpose, and the member's consent to that use may be implied if the member does not contact us.

If a member does not consent to certain uses of personal information, then unfortunately we may not be able to provide the member with some of our products and/or services.

We will comply with the credit reporting provisions of Part IIIA of the Privacy Act 1988 (Commonwealth). If that Part prohibits the collection, use or disclosure of information about a member without the member's consent, we will not collect, use or disclose that information unless and until the member's express consent has been obtained.

8 Marketing Information

We may use our members' personal information, such as their name and address, to provide them with information about the other products and services that are available from us, from our related entities, and from other businesses with which we or our related entities have relationships. With the member's permission we may also use members' personal information to invite them to participate in research, which will assist us in offering products and services that suit our members' financial needs.

In any direct marketing material that we send to our members we will advise them that they can opt out of receiving any more direct marketing material. We will not send any direct marketing material to a member who has notified us that they do not wish to receive such material.

9 Keeping members' personal information accurate, complete, and up-to-date

Our ability to provide our members with the best possible level of service is dependent on us having accurate personal information about them.

We will take all reasonable steps to ensure that our members' personal information is accurate, complete, and up-to-date whenever we collect or use it or are required to disclose it.

If we become aware that the personal information we hold in our records is inaccurate or incomplete, either because a member has contacted us or otherwise, we will correct it as soon as practicable. If a member disagrees with us about whether the personal information is accurate, complete or up-to-date, the member has the right to request that a statement be attached to their personal information claiming that the information is inaccurate, incomplete or out-of-date.

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856

430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

10 Storage of members' personal information

We will take reasonable measures to protect all personal information that we hold from misuse and loss and from unauthorised access, modifications or disclosure.

Only authorised users may access members' personal information, and access is only for approved purposes.

Our members' personal information may be stored as hardcopy documents or as electronic data.

We maintain physical security over our paper and electronic data stores by using locks and security systems and other measures deemed appropriate. We also maintain computer and network security, which includes such measures as firewalls (Internet security measures), and passwords to control access to our computer systems.

We have a documented data risk management system to help maintain the security and integrity of both member and corporate information.

We also maintain a records retention policy which requires that information no longer required be destroyed in a confidential manner. We use a specialist third party document storage organisation to securely store certain hard copy documents until their retention date expires, after which they are confidentially destroyed.

In addition, all employees sign a confidentiality agreement as a condition of their employment.

11 Website security and privacy

The use of the Internet allows us to provide banking and financial services that our members can access whenever it is convenient to them from wherever they have Internet access.

We appreciate that members may have concerns about the confidentiality and security of the personal information that we may collect about them online. In recognition of our members' possible concerns, we have implemented systems to ensure that our online dealings with our members are as secure and confidential as our members' dealings with us in person, or on the telephone.

12 Members' access rights and how to contact us

We will, upon request, provide our members with access to the personal information we hold about them, except to the extent that:

- a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
- b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
- c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- d) the request for access is frivolous or vexatious; or
- e) the information relates to existing or anticipated legal proceedings between us and the member, and the information would not be accessible by the process of discovery in those proceedings; or
- f) providing access would reveal our intentions in relation to negotiations with the member in such a way as to prejudice those negotiations; or
- g) providing access would be unlawful; or
- h) denying access is required or authorised by or under law; or
- i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856

430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

- j) providing access would be likely to prejudice:
 - i. the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - ii. the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - iii. the protection of the public revenue; or
 - 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; by or on behalf of an enforcement body; or
- k) an enforcement body performing a lawful security function asks us not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

If we are not required to provide a member with access to their personal information, we will:

- a) if reasonable, consider whether the use of a mutually agreed intermediary is appropriate; and
- b) advise the member of the reasons for denial of access.

We may recover reasonable costs from a member for supplying them with access to the personal information we hold about them.

To facilitate the provision of information, we will request that our members identify, as clearly as possible, the information they require.

We will respond to our members' requests as soon as is reasonably practicable, taking into account the age, nature and amount of information requested.

To contact us about privacy issues, our members can speak to a consultant at their nearest Personal Financial Centre, telephone us on 13 25 85, email us, or write to the Member Advocate at our mailing address.

13 National Privacy Principles

13.1 Collection

Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, how the person can get access to their personal information, and what happens if the person does not give the information.

The signing of a Privacy Statement covers this requirement along with a simple verbal statement as to why the information is needed e.g. *"In order to assess a loan application Community CPS requires the information requested on this form."* Members will be required to read and sign the Privacy Statement when completing membership application forms. Other application forms contain a short paragraph that refers to the Privacy Statement. The signed Privacy Statement must be attached to the completed membership application form for Community CPS' record keeping purposes. A modified version of the Privacy Statement with a coupon to not receive marketing information is available in the brochure 'Our commitment to your privacy'.

As a general rule, and if it is reasonable and practicable to do so, Community CPS must collect personal information about an individual only from that individual. Community CPS can only collect information that is necessary to effectively pursue a function or activity requested by a member or potential member. Community CPS cannot collect personal information on the off chance that it may become necessary for one of our functions or activities in the future. If a person gives more information than is needed for a requested function or activity, the additional information is not permitted to be kept in case it might be useful in the future.

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856
430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au **Website:** www.unitedcommunity.com.au

13.2 Use & Disclosure

An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.

Community CPS can only use personal information collected for the specific purpose it was collected (primary purpose) eg. opening a membership, assessing a loan application, providing Internet Banking access, etc; and for limited other purposes (secondary purposes) such as reasonably expected purposes, consented purposes, direct marketing, authorised by law and enforcement body activities.

Separate application forms, or clearly marked sections of an application form must be completed by the member when they request more than one product or service.

If a member provides personal information for a Car Loan (primary purpose) and Community CPS requires the Loan to be secured therefore requiring Comprehensive Car Insurance to be taken out, Community CPS staff can inform the member that Community CPS does offer car insurance (secondary purpose) and ask if they would like a quote. However Community CPS cannot inform the member about Building or Contents Insurance unless the member instigates a request for this information as these products are not related to the primary purpose that the member provided the information for. Community CPS can provide a lead-in question, for example: “*Would you like me to provide you with a quote for Building and Contents Insurance?*” If the member agrees to obtain a quote, the member is seen as instigating the request. However, should the member decline, Community CPS cannot proceed any further.

14 Follow up Calls

Follow up telephone calls in respect of a product or service that an individual has specifically applied for (including an insurance quote) is deemed to be ‘reasonably expected’ and therefore is within NPP. The follow up call should only be in respect of the specific product/service that the individual applied for or inquired about and should not be used as an opportunity to cross sell.

14.1 Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to date.

It has always been and will continue to be Community CPS practice to ensure that all member information it collects, uses, or discloses is accurate, complete, and up-to-date.

14.2 Data Security

An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.

Access to PCs and computer systems is password protected and limited to authorised security levels. Hard copy member personal information is stored in a secure manner and destroyed in line with legislative requirements. A clean desk policy is promoted along with a general awareness of privacy of information displayed on screens and verbalised in public areas. All paper files, letters, correspondence, memos etc that contain personal information must be shredded or placed in a secure waste disposal bin.

14.3 Openness

An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.

The Community CPS Privacy Policy is accessible to members via the Community CPS website and available to members or other interested persons on request.

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856

430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

14.4 Access & Correction

Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.

The Community CPS Privacy Policy makes it very clear that members or other persons may request access to their personal information that Community CPS may hold. A *Request for Personal Information* form has also been introduced to assist with this requirement. Individuals must be given access to all information held that falls within the definition of personal information including information collected from third parties, unsolicited information that has been recorded and opinions about an individual that have been recorded.

If a member identifies incorrect or incomplete information being held by Community CPS they can request the information is updated and generally that would be Community CPS' practice. In circumstances where the individual and Community CPS disagree about whether or not the information is accurate, complete or up-to-date the individual can provide a statement claiming the information is not accurate, complete or up-to-date and Community CPS must attach this statement to the individual's record.

Access is to personal information only, not to evaluative information in connection with commercially sensitive decision making processes. In most cases, access in these circumstances is sought to try and find out why an adverse decision has been made. These concerns can be met by explaining the reasons for the decision i.e. *"you did not pass our risk assessment process"* or *"the combination of your liabilities and employment history meant that you did not meet our lending criteria"*.

15 Fee for retrieval of information

Community CPS can charge a fee for providing access to personal information, where complying with a request for access imposes substantial costs on the organisation. Community CPS is not entitled to charge an individual for the lodgement of a request for access to their personal information.

Community CPS has determined that 'generally' a flat fee will be apply for each Request for Personal Information form completed, and each form will cover one membership only. Individuals can request information pertaining to more than one matter related to the membership on the one form for the one fee (i.e. Membership, Loan Application, Term Deposit, Insurance etc).

If an individual requests personal information applicable to two memberships then two Request for Personal Information forms should be completed and this should be regarded as two separate requests. However there will be instances where the membership that the personal information requested relates to may not be clear cut, thus discretion will be required to determine if it is one query or more.

Requests for personal information from companies Community CPS has alliances with may incur costs from both Community CPS and the alliance company, depending on the information being requested. That is, if a member requests insurance information held with Community CPS and Allianz then the Community CPS fee would apply (Allianz do not charge a fee). Similarly requests for information from Community CPS and Medibank Private would incur the Community CPS \$25.00 fee and the Medibank Private fee (hourly rate plus a minimum charge).

United Community

A Division of Community CPS Australia Limited ABN 15 087 651 143 AFSL 237856
430 Roberts Road Subiaco WA 6008, P.O. Box 882 Subiaco WA 6904. Telephone: 13 25 85 Facsimile: (08) 9381 4741

Email: member@unitedcommunity.com.au Website: www.unitedcommunity.com.au

16 Requesting personal information via the telephone

Under the current Telephone Banking Passcode system, a Telephone Banking Passcode is not considered 'adequate' ID to enable a request for personal information to be initiated. It may be a signatory that is using the Telephone Banking Passcode (as the current system is one Passcode per membership) which means that the potential exists for someone other than the member to request personal information regarding the member. Only transactional type information can be provided using a Telephone Banking Passcode and low security information can be updated such as address, telephone number etc.

When a request for personal information is received via the telephone, advise the person that if they wish to proceed we suggest they visit a PFC and discuss their concerns with a Consultant who may be able to provide them information immediately. Alternatively we can send them a *Request for Personal Information* form to be completed and returned to Community CPS.

16.1 Identifiers

Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government 'agency'.

Community CPS does not and will not use an identifier that has been assigned by a Commonwealth Government Agency as a means of identifying members. Community CPS uses a Relationship Information Manager (RIM) number (or membership number) to uniquely identify each member. This number is generally sequential, based on the date a person becomes a member of Community CPS, i.e. the most recent member will have the highest RIM number.

16.2 Anonymity

Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do.

In most situations a member or potential member will be required to provide personal information if Community CPS is to assess their application for membership or other products or services.

In cases of a general inquiry, Community CPS does not require any personal information about the individual. However if the individual wishes Community CPS to mail them information they may give their membership number, at which time anonymity is removed and standard practice applies (load details in MRMS and follow up call). If the individual just provides their name and address then staff cannot search and locate a membership Number, load data into MRMS and give a follow-up call without the individuals consent.

16.3 Transborder Data Flows

An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.

Community CPS does transfer members' funds to recipients in a foreign country but this is only done with the member's express consent.

Traveler SWIFT and National Bank Telegraphic Transfers both come under this principle and are only done with the member's expressed consent. Both are large international organisations operating with comparable information privacy schemes globally.

16.4 Sensitive Information

An organisation must not collect sensitive information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety.

Sensitive information is defined to include health information and personal information that also contains information or an opinion about sensitive subjects, such as an individual's political opinions, religious beliefs or sexual preferences or practices.

There are not many situations where Community CPS requires sensitive information to be collected. Where it is required the relevant application form will contain the appropriate request for consent (e.g. Medibank Private Health Insurance application – this information is not recorded by Community CPS as it is forwarded directly to Medibank Private).

Community CPS staff should not view medical information. However, should they do so, they cannot record or make any judgement based on this information. That is, a Loan can not be assessed on information and knowledge that was not given with the member's consent.

When photocopying a Drivers Licence, references to Organ Donors must be blacked over.

17 Provision of Information to Third Party Organisations

From time to time Community CPS may be required to provide details of the personal information of its members (customers) or staff to a third party under an alliance, contractual, or other arrangement. Whenever personal information is being provided by Community CPS to a third party, it is imperative that this information is handled in accordance with the Privacy Act and the National Privacy Principles.

Staff must ensure that any arrangement with a third party which requires the provision of members (customers) or staff personal information contains a suitable privacy clause. The clause must specify that the third party must comply with Privacy Act and National Privacy Principles when dealing with any personal information provided by Community CPS. In instances where a third party is not bound by the Privacy Act and National Privacy Principles (i.e. they are a small business with turnover of \$3m or less) the clause must specify that the third party must comply with the Privacy Act and National Privacy Principles as though they were bound by it.

Note that the wording of any arrangement and the clauses contained therein must receive legal signoff by Community CPS' General Legal Council.

Upon the expiration or cancellation of any alliance, contractual, or other arrangement with a third party, written confirmation must be sought to confirm that any personal information provided by Community CPS has either been returned, destroyed or permanently de-identified. This is required to ensure compliance with NPP 4.2 as the personal information is no longer required by the third party.